ICOM

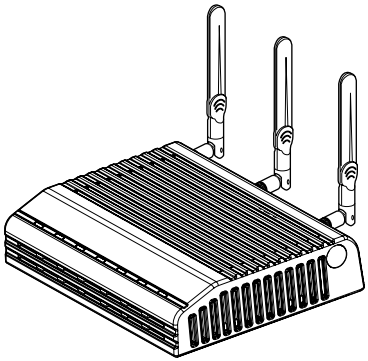
取扱説明書

WAVEMASTER®

WIRELESS ACCESS POINT

AP−80

[IEEE802.11n]規格準拠
[IEEE802.11a(W52/W53/W56)/b/g]規格準拠
[IEEE802.3af]規格PoE準拠



Icom Inc.

ご使用になる前に 1
接続ガイド 2
無線LANの詳細設定 3
そのほかの基本設定 4
設定画面について 5
保守について 6
ご参考に 7

5.2/5.3GHz帯無線LANの使用は、
電波法により、屋内に限定されます。

はじめに

このたびは、本製品をお買い上げいただきまして、まことにありがとうございます。

本製品は、[IEEE802.11a(W52/W53/W56)]規格★1.、[IEEE802.11b/g]規格★2.、[IEEE802.11n]規格★3.に準拠したワイヤレスアクセスポイントです。

ご使用の前に、この取扱説明書をよくお読みいただき、本製品の性能を十分発揮していただくとともに、末長くご愛用くださいますようお願い申し上げます。

★1.[IEEE802.11a]規格の無線LANについて
[IEEE802.11a(W52/W53)]:5.2/5.3GHz帯の無線LAN規格
[IEEE802.11a(W56)] :5.6GHz帯の無線LAN規格
※本製品は、[IEEE802.11a(J52)]規格に準拠していません。

★2.[IEEE802.11g]規格の無線LANについて
[IEEE802.11b]規格の無線LANと互換性があります。
[IEEE802.11]規格(14CH)に準拠していません。

★3.[IEEE802.11n]規格の無線LANについて
[IEEE802.11a/b/g]規格と互換性があります。

5.2/5.3GHz帯無線LANの使用は、電波法により、屋内に限定されます。

登録商標/著作権について

アイコム株式会社、アイコム、Icom Inc.、アイコムロゴ、WAVEMASTERは、アイコム株式会社の登録商標です。
Microsoft、Windows、Windows Vistaは、米国Microsoft Corporationの米国およびその他の国における登録商標です。
Adobe、Adobe Readerは、Adobe Systems Incorporated(アドビシステムズ社)の登録商標です。
Atherosは、Atheros Communications, Inc.の登録商標または商標です。
Wi-Fi、WPA、WPSは、Wi-Fi Allianceの商標または登録商標です。
FOMAは、株式会社NTTドコモの登録商標です。
その他、本書に記載されている会社名、製品名は、各社の商標および登録商標です。
本製品は、GoAhead Software社のGoAhead WebServerソフトを含んでいます。
© 2002 GoAhead Software, Inc. All Rights Reserved.

無線LAN規格について

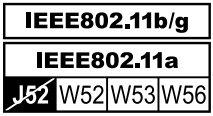
本製品が準拠する無線LAN規格と最大通信速度の関係は、以下のとおりです。

本製品が準拠する無線LAN規格	周波数帯	帯域幅モード	最大通信速度(理論値)★
[IEEE802.11n (W52)]	5.2GHz	20MHz	130Mbps
		40MHz	300Mbps
[IEEE802.11n (W53)]	5.3GHz	20MHz	130Mbps
[IEEE802.11n (W56)]	5.6GHz	20MHz	130Mbps
[IEEE802.11n]	2.4GHz	20MHz	130Mbps
		40MHz	300Mbps
[IEEE802.11a (W52/W53)]	5.2GHz/ 5.3GHz	20MHz	54Mbps
[IEEE802.11a (W56)]	5.6GHz	20MHz	54Mbps
[IEEE802.11g]	2.4GHz	20MHz	54Mbps
[IEEE802.11b]	2.4GHz	20MHz	11Mbps

★最大通信速度は、実際のデータ転送速度(実測値)を示すものではありません。
※本製品の出荷時や設定を初期化したときは、[IEEE802.11n/b/g]規格で通信します。
※[IEEE802.11n/b/g]規格と[IEEE802.11n/a(W52/W53/W56)]規格の同時通信には対応していません。

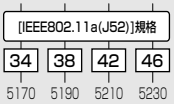
[IEEE802.11a(W52/W53/W56)]規格の無線通信チャンネルについて

右に記載する記号がある製品は、[IEEE802.11a(W52/W53/W56)]規格で採用された無線通信チャンネルに対応した製品を意味します。
無線LAN端末についても、右に記載する記号がある製品でご使用いただくことをおすすめします。
※右の記号は、本製品のシリアルシールにも記載されています。



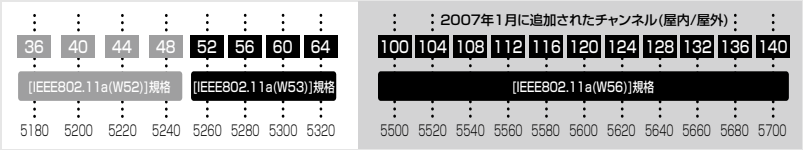
[IEEE802.11a]規格の周波数(MHz)

2005年5月以前の無線LAN規格



[IEEE802.11a(J52)]規格の無線LANが本製品の近くで稼働している環境で、本製品の[IEEE802.11n/a(W52)]規格をご使用になると電波干渉の原因になりますので、ご注意ください。

2005年5月以降の無線LAN規格



[IEEE802.11a(W52/W53)]規格の範囲　　[IEEE802.11a(W56)]規格の範囲

はじめに

本製品の概要について

◎ [IEEE802.11a(W52/W53/W56)]規格、[IEEE802.11b/g]規格に加え、[IEEE802.11n]規格に準拠しています。
※[IEEE802.11n]規格は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。
※[IEEE802.11a(J52)]規格の無線LAN端末とは通信できません。

◎ [IEEE802.11n]規格は、2倍の周波数帯域幅と複数のアンテナを使用してデータを同時に送受信することで、最大300Mbps(理論値)の速度で通信できます。
また、[IEEE802.11a(W52/W53/W56)/b/g]規格とも互換性がありますので、既存の無線ネットワークと通信できます。

◎異なる無線LAN規格の機器を同時に使用する環境において、[IEEE802.11n/a(W52/W53/W56)/b/g]規格の速度低下を緩和するプロテクション機能を搭載しています。

◎DFS機能の搭載により、5.3/5.6GHz帯[IEEE802.11n/a(W53/W56)]規格で通信しているときは、気象レーダーなどによる電波干渉を自動で回避します。

◎ [IEEE802.1Q]のVLAN規格に準拠した仮想AP機能を搭載していますので、本製品1台で最大4グループの無線ネットワークを構築できます。

◎ネットワーク認証は、「共有キー」、「オープンシステム」、「IEEE802.1X」、「WPA」、「WPA2」、「WPA-PSK」、「WPA2-PSK」に対応しています。
「WPA」、「WPA2」、「IEEE802.1X」を設定すると、認証にRADIUSサーバーを使用できます。

◎ [IEEE802.3af]に準拠したPoE受電機能に対応していますので、弊社別売品の「イーサネット電源供給ユニット(SA-4)」、または[IEEE802.3af]規格対応のHUB(市販品)から電源を供給できます。

◎「Wi-Fiアライアンス」が提唱するWPS(Wi-Fi Protected Setup)機能の搭載により、SSIDと暗号化(WPA-PSK/WPA2-PSK)を本製品(仮想AP:ath0～ath3)、およびWPS機能対応の無線LAN端末に自動設定できます。
※2009年11月現在、本製品は、Wi-FiアライアンスよりWPS認定されていません。

◎有線LANは、10BASE-T/100BASE-TX/1000BASE-Tの自動切り替えに対応し、ポートの極性についても、MDI(ストレート)/MDI-X(クロス)を自動判別します。

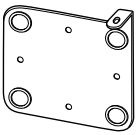
◎ネットワーク管理機能として、SNMPをサポートしています。

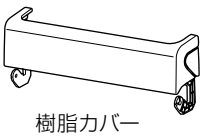
◎技術基準適合証明を取得していますので、無線局の免許は不要です。

別売品について

（2009年11月現在）

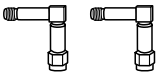
MB-119
壁面取付金具(磁石/樹脂カバー付属)


壁面プレート

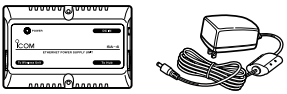

樹脂カバー

磁石

AD-117
L型アンテナコネクター


L型コネクター　I型コネクター

SA-4
イーサネット電源供給ユニット



OPC-1402 設定用ケーブル
〈シリアル通信用(約1m)〉

RS-AP2
アクセスポイント
集中管理ツール

【別売品についてのご注意】

弊社製別売品は、本製品の性能を十分に発揮できるように設計されていますので、必ず弊社指定の別売品をお使いください。

弊社指定以外の別売品とのご使用が原因で生じるネットワーク機器の破損、故障あるいは動作や性能については、保証対象外とさせていただきますので、あらかじめご了承ください。

はじめに

出荷時のおもな設定値について

ネットワーク設定	LAN側IP	IPアドレス設定	IPアドレス:	192.168.0.1
			サブネットマスク:	255.255.255.0
	DHCPサーバー	DHCPサーバー設定	DHCPサーバー機能を使用:	しない
無線設定	無線LAN	無線LAN設定	無線UNITを使用:	する
			チャンネル:	001CH（2412MHz）
	仮想AP（ath0）	仮想AP設定	SSID:	WAVEMASTER-0
		暗号化設定	暗号化方式:	なし
	WPS	WPS設定	使用するインターフェース:	なし
システム設定	管理者	管理者パスワードの変更	管理者ID:	admin（変更不可）
			現在のパスワード:	wavemaster (半角小文字)

※上記以外の設定値については、本書172ページ～173ページをご覧ください。
「ath0」は、出荷時に設定されている仮想AP（アクセスポイント）の名称です。

本書の表記について

本書は、次の表記規則にしたがって記述しています。

「　」表記 ：オペレーティングシステム（OS）の各ウィンドウ（画面）、ユーティリティー、設定画面の各メニューとそのメニューに属する設定画面の名称を（「」）で囲んで表記します。

［　］表記 ：タブ名、アイコン名、テキストボックス名、チェックボックス名、各設定画面の設定項目名を（［］）で囲んで表記します。

〈　〉表記 ：ダイアログボックスのコマンドボタンなどの名称を（〈〉）で囲んで表記します。

※ Microsoft® Windows Vista® Home Basic、Microsoft® Windows Vista®Home Premium、Microsoft® Windows Vista® BusinessおよびMicrosoft® Windows Vista® Ultimateは、Windows Vistaと表記します。
Microsoft® Windows® XP Professional、Microsoft® Windows® XP Home Editionは、Windows XPと表記します。
Microsoft® Windows® 2000 Professionalは、Windows 2000と表記します。
Microsoft® Windows® Millennium Editionは、Windows Meと表記します。
Microsoft® Windows® 98 Second Editionは、Windows 98 SEと表記します。

※本書は、Ver 2.05のファームウェアを使用して説明しています。

※ 本書では、紙面上の都合により、設定画面の一部を省略して掲載しています。

※ 本書中の画面は、OSのバージョンや設定によって、お使いになるパソコンと多少異なる場合があります。

ご使用までの流れ

本製品を設定されるときは、次の手順にしたがってお読みください。
順番に基本的な設定ができる構成になっています。
※右端に記載する数字は、本書の参照ページです。

Step. 1	ご注意と保守について/接続ガイド	**別紙**
Step. 2	本製品のおもな機能	16ページ～22ページ
Step. 3	無線通信までの基本設定手順	23ページ～44ページ
Step. 4	仮想AP機能など、無線LANの詳細設定	45ページ～58ページ
Step. 5	内部時計など、その他の基本設定	59ページ～62ページ
Step. 6	設定内容の書き込みや保存のしかた	158ページ、159ページ
Step. 7	本製品の設定を初期化するには	160ページ、161ページ
ご参考に	困ったときは	166ページ～168ページ

もくじ

はじめに ―― 2
登録商標/著作権について …… 2
無線LAN規格について …… 3
本製品の概要について …… 4
別売品について …… 5
出荷時のおもな設定値について …… 6
本書の表記について …… 6
ご使用までの流れ …… 7

第1章 ご使用になる前に ―― 11
1. 各部の名称と機能 …… 12
2. 付属品の取り付けかた …… 14
3. 本製品のおもな機能 …… 16

第2章 接続ガイド ―― 23
Step1. 設定に使うパソコンの用意 …… 24
Step2. 固定IPアドレスを設定する …… 26
Step3. 設定に使うパソコンの接続 …… 30
Step4. 設定画面へのアクセスを確認する …… 37
Step5. 本体IPアドレスを変更する …… 38
Step6. 無線ネットワーク名を設定する …… 39
Step7. 暗号化を設定する …… 40
Step8. WPS機能を有効にする …… 41
Step9. 〈WPS〉ボタンで自動設定を開始する …… 42

第3章 無線LANの詳細設定 ―― 45
1. [IEEE802.11n/a]規格で無線通信するには …… 46
2. [WEP RC4]暗号化を設定するには …… 47
3. 自動設定したいSSIDと共有鍵(キー)を指定するには …… 52
4. 仮想APを設定するには …… 56
5. MACアドレスフィルタリングを設定するには …… 58

第4章 そのほかの基本設定 59

1. 設定画面へのアクセスを制限するには 60
2. 内部時計を設定するには 61
3. 本製品のDHCPサーバー機能を使用するには 62

第5章 設定画面について 63

1. 設定画面の名称と機能 65
2.「LAN側IP」画面 66
3.「DHCPサーバー」画面 69
4.「ルーティング」画面 73
5.「パケットフィルター」画面 75
6.「無線LAN」画面 96
7.「仮想AP」画面 104
8.「認証サーバー」画面 118
9.「MACアドレスフィルタリング」画面 120
10.「WMM詳細」画面 127
11.「ARP代理応答」画面 134
12.「WPS」画面 137
13.「管理者」画面 143
14.「時計」画面 144
15.「SYSLOG」画面 147
16.「SNMP」画面 148
17.「ネットワーク情報」画面 149
18.「SYSLOG」画面 150
19.「無線LANユニット」画面 151
20.「端末情報」画面 153

もくじ

第6章 保守について ―― 157

1. 設定内容の確認または保存 …… 158
2. 保存された設定の書き込み …… 159
3. 設定を出荷時の状態に戻すには …… 160
4. ファームウェアをバージョンアップする …… 162

第7章 ご参考に ―― 165

1. 困ったときは …… 166
2. Telnetで接続するには …… 169
3. 設定項目の初期値一覧 …… 172
4. 設定画面の構成について …… 174
5. PoEによる電源供給について …… 176
6. 対応無線LAN製品について …… 177
7. 暗号化対応表 …… 178

ご使用になる前に

第1章

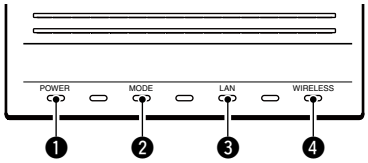
この章では、
本製品のおもな機能などを説明しています。

1. 各部の名称と機能 …… 12
　上面部 …… 12
　後面部 …… 13
2. 付属品の取り付けかた …… 14
　マスクシートの取り付け …… 14
　アンテナの取り付け …… 15
3. 本製品のおもな機能 …… 16
　アクセスポイント機能について …… 16
　無線LANセキュリティー …… 17
　ローミング機能 …… 18
　無線ネットワーク名(SSID)について …… 19
　接続端末制限機能 …… 19
　[IEEE802.11n]規格 …… 19
　PoE機能について …… 20
　仮想AP機能…… 21
　WPS機能…… 22

1. 各部の名称と機能

上面部

各ランプの動作と状態について説明します。



❶ [POWER]ランプ ……電源と初期化操作(☞P160)の状態を表示します。
- 点灯: 本製品の電源が入っているとき
- 点滅: 起動中、または設定初期化のため、〈MODE〉ボタンを操作したとき

❷ [MODE]ランプ ……WPS機能(☞P22、P42)による暗号化自動設定の状態を表示します。
- 点灯: 設定を完了したとき
- 消灯: 設定完了後、5分経過したとき
  設定失敗後、20秒経過したとき
- 点滅: 設定中(緑色)、または設定を失敗(赤色)したとき
  ※設定中は、ゆっくり点滅(緑色)し、2分経過すると、設定失敗となり赤色で点滅します。

❸ [LAN]ランプ ……有線LANの状態を表示します。
- 点灯: LANケーブルの接続が正常なとき
- 消灯: LANケーブルが未接続のとき
- 点滅: データを送受信しているとき

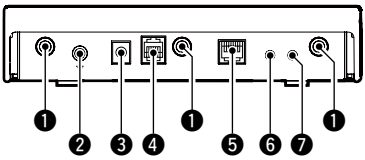
❹ [WIRELESS]ランプ ……無線LANの状態を表示します。
- 点灯: 本製品と無線通信を確立したとき
- 消灯: 本製品と無線通信が確立していない、または4分～5分以上、無線通信しない状態がつづいたとき
- 点滅: DFS機能が動作したとき(☞接続ガイド:別紙)

【ご参考に】

ファーム更新中は、すべてのランプ(❶～❹)が同時に点灯します。
電源を入れたときは、すべてのランプ(❶～❹)が1回点灯後、[POWER]ランプだけが点滅します。

後面部

接続各部と各ボタンの名称について説明します。



❶アンテナコネクター ……付属のアンテナを接続します。
※十分な性能でご使用いただくため、アンテナは、必ず3本とも接続してください。

❷アース端子 ……アース線(市販品)を接続します。

❸DCジャック ……付属のACアダプターを接続します。
※本製品の[LAN]ポートに、イーサネット電源供給ユニット(別売品:SA-4)、または[IEEE802.3af]規格対応のHUBを接続するときは、付属のACアダプターを接続する必要はありません。

❹[CONSOLE]ポート(RJ-11型×1) ……RS-232Cシリアルインターフェース搭載の制御機器と接続して、本製品を設定するとき使用します。
※接続には、設定用ケーブル(別売品:OPC-1402)が必要です。

❺[LAN]ポート(RJ-45型×1) ……LANケーブル(市販品)を使用して、HUBなどのネットワーク機器と接続します。
※[1000BASE-T]規格でご使用になる場合、カテゴリー5e以上のLANケーブルをご使用ください。

❻〈MODE〉ボタン ……設定を初期化するとき使用します。(☞P160)
※指で押せないときは、ペン先などを利用して押してください。

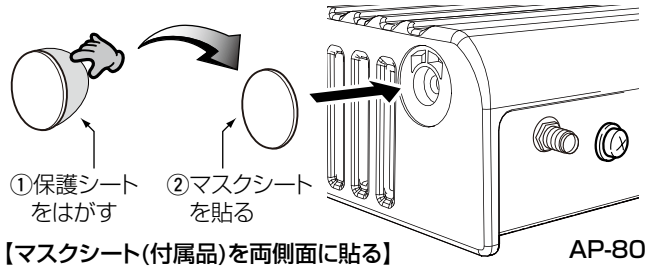
❼〈WPS〉ボタン ……WPS機能を使用するとき使用します。(☞P22)
※出荷時、または全設定を初期化したときは、WPS機能の操作が「無効」に設定されています。
※指で押せないときは、ペン先などを利用して押してください。

2. 付属品の取り付けかた

マスクシートの取り付け

マスクシートを下図のように本製品の両側面に貼り付けます。

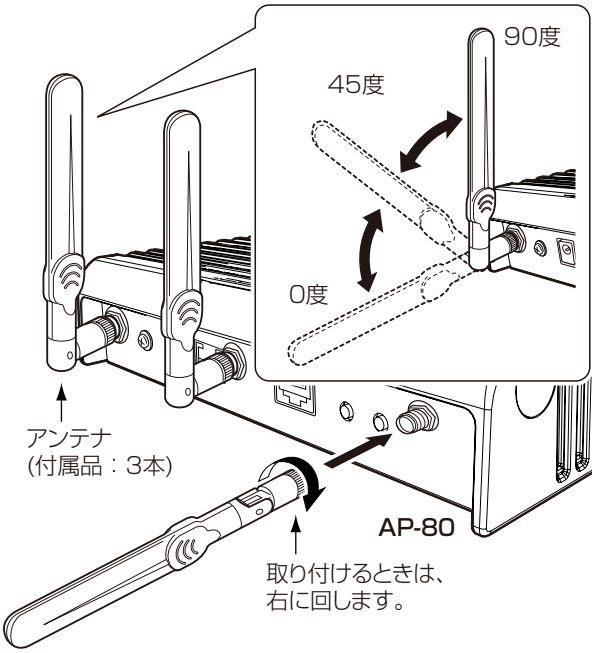
※MB-119(別売品)に付属する樹脂カバーを本製品に取り付ける場合は、本製品に取り付けた樹脂カバーをビスで固定するまで、マスクシートを貼り付けないでください。



【マスクシート(付属品)を両側面に貼る】 AP-80

アンテナの取り付け

取り付けるときは、アンテナの根元を右方向に手で締まる程度まで回します。
アンテナは、3段階の角度(0/45/90度)に折り曲げて使用できます。
また、折り曲げた状態で、左右に回転できます。
取りはずすときは、アンテナの根元を持って左方向に回します。
※十分な性能でご使用いただくため、アンテナ(付属品)は、3本とも取り付けてください。
※電波状況が悪いと感じられたときは、アンテナの向き、または設置場所を変更してください。
※AD-117(別売品)を本製品に取り付ける場合は、AD-117の取扱説明書にしたがってアンテナを接続してください。



⚠警告

本製品に取り付けたアンテナを持って本製品を振り回さないでください。
本人やほかの人に当たるなどして、けがや破損、および故障の原因になります。

【ご注意】

技術基準適合証明を取得していますので、弊社指定以外のアンテナは使用できません。

3. 本製品のおもな機能

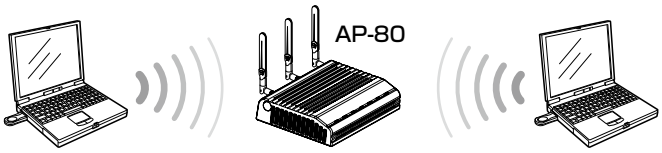
アクセスポイント機能について

本製品は、[IEEE802.11n/a(W52/W53/W56)/b/g]規格の無線アクセスポイントとして機能します。

※出荷時、本製品は、[IEEE802.11n/b/g]規格の無線LAN端末と通信します。

※[IEEE802.11n/b/g]規格と[IEEE802.11n/a(W52/W53/W56)]規格の同時通信には、対応していません。

※[IEEE802.11]規格(14CH)の無線LAN端末とは通信できません。



【例】 [IEEE802.11g]規格の「001CH」で通信する無線LAN端末

同時に使用できる無線LAN端末の台数について

本製品に多くの無線LAN端末が同時にアクセスすると、通信速度が著しく低下することがあります。同時に使用できる無線LAN端末の台数は、接続端末制限機能(☞P19、P107)で仮想APごとに制限(最大63台)されますが、全仮想AP(ath0～ath3)の合計が10台を超えないように運用されることをおすすめします。

異なる無線LAN規格の混在による電波干渉で、[IEEE802.11n]規格の通信速度が著しく低下する場合は、[プロテクション機能](☞P103)と併せてご使用ください。

無線LANセキュリティー

本製品は、無線LAN通信に必要な次のセキュリティーを搭載しています。
詳細については、本書5章をご覧ください。

※対応する弊社製無線LAN製品について詳しくは、本書7章をご覧ください。

- **MACアドレスフィルタリング**
  あらかじめ本製品の各仮想AP(ath0～ath3)に登録されたMACアドレスを持つ無線LAN端末だけにアクセスを許可、または拒否するとき使用します。

- **WEP RC4**※1
  無線通信で一般によく使用されるセキュリティーです。
  無線ネットワーク間で送受信するデータを、設定された文字列を元に暗号化して安全性を確保します。

- **TKIP/AES**※2
  Windows Vista、Windows XP(Service Pack1)に修正プログラムを適用、またはWindows XP(Service Pack2以降)のパソコンで使用できる暗号化方式です。

- **WPA/WPA2**
  RADIUSサーバーで「IEEE802.1X」認証します。

- **WPA-PSK/WPA2-PSK**
  RADIUSサーバーを使用しない簡易的な認証方式で、共有鍵(キー)を使用します。

- **IEEE802.1X**※3
  RADIUSサーバーを使用して、無線LAN端末からのアクセスにユーザー認証を設ける機能です。

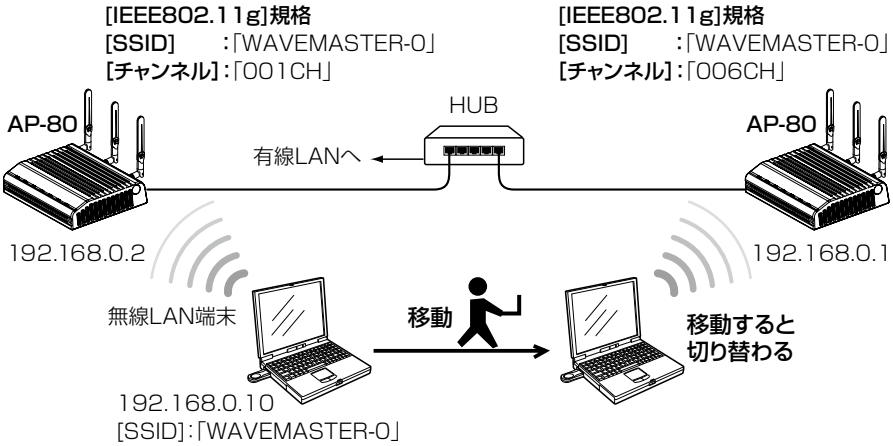
※1 通信相手と暗号化方式や鍵(キー)の設定が異なるときは、通信できません。
※2 「TKIP」は、「WEP RC4」より強力な暗号化方式です。
「AES」は、「TKIP」より強力な暗号化方式です。
[IEEE802.11n]規格は、暗号化方式を「なし」または「AES」に設定している場合に有効です。
※3 WEP RC4以外の暗号化方式では使用できません。

【ご注意】
Windows XPやWindows Vistaを使用する無線LAN端末は、「WEP RC4 152(128)」の暗号化セキュリティーには対応していません。

3. 本製品のおもな機能

ローミング機能

無線LAN端末を移動させても、自動的に電波の状況のよい無線アクセスポイント（本製品）に切り替えることによって、工場など広い場所で無線LANが利用できる機能です。



ローミング機能を使用するには

◎ 有線LANに接続する本製品と無線LAN端末は、無線ネットワーク名（SSID）や暗号化をすべて同じ設定にしてください。

◎ DHCPサーバー機能が「有効」に設定された本製品などが同一ネットワーク内に複数存在すると、IPアドレスが重複して不測の事態になりますので、接続にはご注意ください。
※出荷時、本製品のDHCPサーバー機能は、「無効」に設定されています。

◎ 本製品に多くの無線LAN端末、または異なる無線LAN規格の端末が混在する環境でご使用になる場合は、電波干渉しないチャンネルを設定してください。
上記の例で使用する無線LAN規格（IEEE802.11g）では、相手側と4チャンネル以上空けて設定してください。
各無線LAN規格での電波干渉を回避するための説明については、[チャンネル:]欄（☞P97～P102）、および[プロテクション機能:]欄（☞P103）をご覧ください。

無線ネットワーク名(SSID)について

本製品と無線LAN端末には、接続先を識別するための無線ネットワーク名として、SSID(またはESS ID)が設定されています。(☞P39、P105)

※異なる[SSID]を設定している無線LAN端末は接続できません。

※無線LAN端末側で「ANY」に設定されていると、本製品の[SSID]の設定に関係なくこの無線LAN端末から接続できます。
「ANY」に設定されている無線LAN端末からの接続を拒否する場合、[ANY接続拒否]を「する」に変更してください。(☞P106)
[ANY接続拒否]とWPS機能(☞P22、P41)との併用は、できません。

※仮想AP機能(☞P21、P56)を使用する場合、同じ[SSID]を各仮想APに設定できません。

接続端末制限機能

本製品の仮想APごとに同時接続できる無線LAN端末の台数を制限して、接続が集中するときに起こる通信速度の低下を防止する機能です。(☞P107)

※出荷時、仮想APごとに最大63台に設定されていますが、全仮想AP(ath0～ath3)の合計が10台を超えないように運用されることをおすすめします。

[IEEE802.11n]規格

2倍の周波数帯域幅と複数のアンテナを使用してデータを同時に送受信することで、最大300Mbps★(理論値)の速度で通信できます。

★[IEEE802.11n]規格は、暗号化方式を「なし」または「AES」に設定している場合に有効です。
さらに、最大300Mbps(理論値)で使用するには、5.2/2.4GHz帯のチャンネルで、「40MHz帯域幅モード」(☞P97)を設定してください。

※[IEEE802.11a(W52/W53/W56)/b/g]規格と互換性があります。

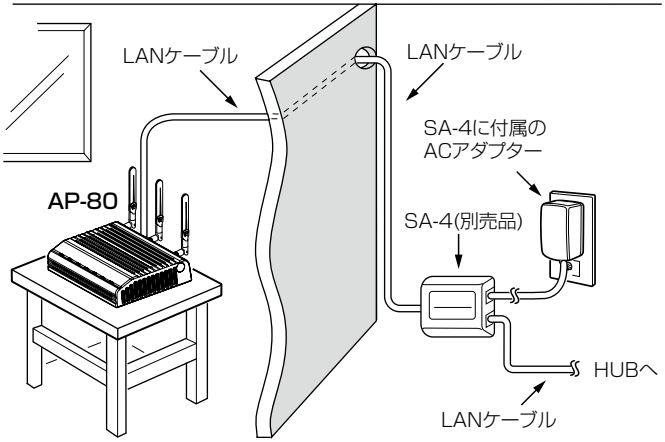
※速度と通信距離については、別紙の「接続ガイド」をご覧ください。

3. 本製品のおもな機能

PoE機能について

本製品の設置場所付近にコンセントや[IEEE802.3af]規格対応のHUBがない場合に備えて、別売品のイーサネット電源供給ユニット(SA-4)をご用意しています。
SA-4をお使いいただくことで、本製品の[LAN]ポートから電源を受電できます。

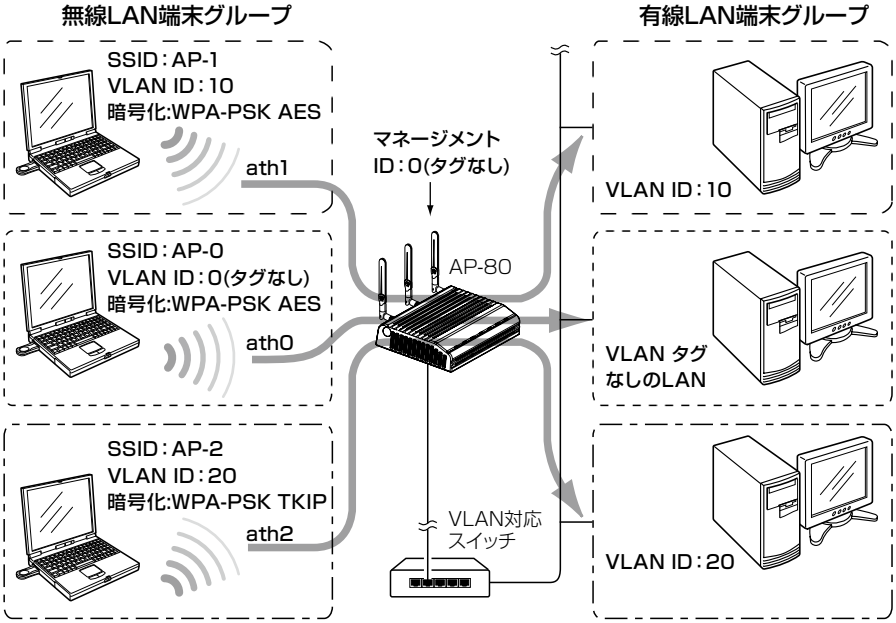
※接続について詳しくは、SA-4に付属の取扱説明書をご覧ください。



仮想AP機能

本製品1台で、条件（SSID/暗号化認証/暗号化方式/VLAN ID）の異なる無線LAN端末グループを複数構成できます。

※下記の図は、「ath0」～「ath2」を異なる無線LAN端末グループの仮想APとして使用する例です。
設定例については、本書56ページをご覧ください。



仮想AP機能を使用するには

◎ 各仮想AP（ath0～ath3）の無線LAN端末グループには、VLAN ID（0～4094）を設定できます。
◎ [SSID]がほかの仮想APと重複する場合は、登録できません。
◎ 最大4グループ（ath0～ath3）の仮想APを使用できます。
◎ Windows XP（Service Pack適用済み）やWindows Vista標準のワイヤレスネットワーク接続（ゼロコンフィグレーション）を使用して、「WEP RC4」で暗号化された本製品と通信する場合、無線LAN端末側のキーインデックスを「1」に設定してください。
◎ 出荷時、本製品の[マネージメントID：]が「0」に設定されていますので、VLAN IDが設定されたネットワークからは、本製品の設定画面にアクセスできません。

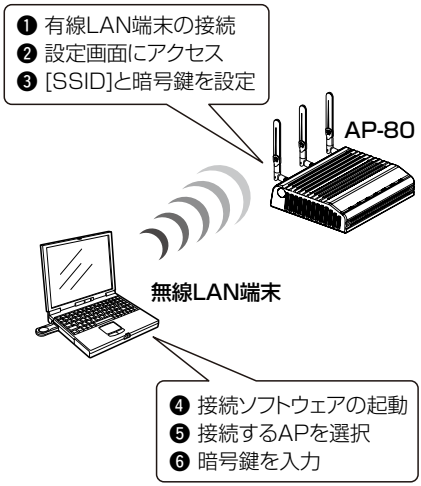
3. 本製品のおもな機能

WPS機能

「Wi-Fiアライアンス」が提唱する機能で、SSIDと暗号化(WPA-PSK/WPA2-PSK)を本製品とWPS機能対応無線LAN端末に自動設定できます。

※自動設定の方法は、本製品の後面パネルにある〈WPS〉ボタンを使用する「プッシュボタン(Push Button Configuration)方式」と自動設定する相手のPINコードが必要な「PIN(Personal Identification Number)方式」を選択できます。
WPS機能による自動設定の例については、本書2章をご覧ください。
WPS機能で無線LAN端末に自動設定したいSSIDと共有鍵(キー)を指定する場合の操作例については、本書3章をご覧ください。

【WPS機能を使用しない場合】



【WPS機能を使用する場合】

WPS機能を使用するには

◎ WPS機能対応の無線LAN端末を準備してください。
◎ 本製品のWPS機能で自動設定する仮想APのインターフェース名称(ath0～ath3)を「WPS」画面にある[使用するインターフェース]欄から選択し、そのインターフェース名称に対するWPS機能を有効に(☞P41)してください。
[使用するインターフェース]欄で仮想APのインターフェース名称が「なし」(出荷時の設定)に設定されている場合は、本製品の後面パネルにある〈WPS〉ボタンを使用できません。
また、本製品の設定画面にも〈開始〉ボタンが表示されません。

接続ガイド

第2章

この章では、
本製品をご使用いただくために必要な基本設定の手順を説明しています。

Step1. 設定に使うパソコンの用意 …… 24
有線LAN端末と接続して設定する場合 …… 24
無線LAN端末と接続して設定する場合 …… 25
Step2. 固定IPアドレスを設定する …… 26
Windows Vistaの場合 …… 26
Windows XP場合 …… 28
Step3. 設定に使うパソコンの接続 …… 30
有線LAN端末を使用する場合 …… 30
無線LAN端末(Windows Vista)を使用する場合 …… 31
無線LAN端末(Windows XP)を使用する場合 …… 34
Step4. 設定画面へのアクセスを確認する …… 37
設定画面にアクセスするには …… 37
Step5. 本体IPアドレスを変更する …… 38
Step6. 無線ネットワーク名を設定する …… 39
Step7. 暗号化を設定する …… 40
Step8. WPS機能を有効にする …… 41
Step9. 〈WPS〉ボタンで自動設定を開始する …… 42

DHCPサーバー機能について

出荷時や全設定初期化時、本製品のDHCPサーバー機能は「無効」、IPアドレスは「192.168.0.1」に設定されています。
本製品を既存のネットワークに接続して使用する場合には、使用状況にあわせて設定を変更してください。

HUBとの接続について

100BASE-TXより低速なHUBは、意図しない動作で通信に障害を与えるなど、通信速度低下の原因になりますので、接続しないでください。

Step1. 設定に使うパソコンの用意

本製品の設定に使用するパソコンを用意します。

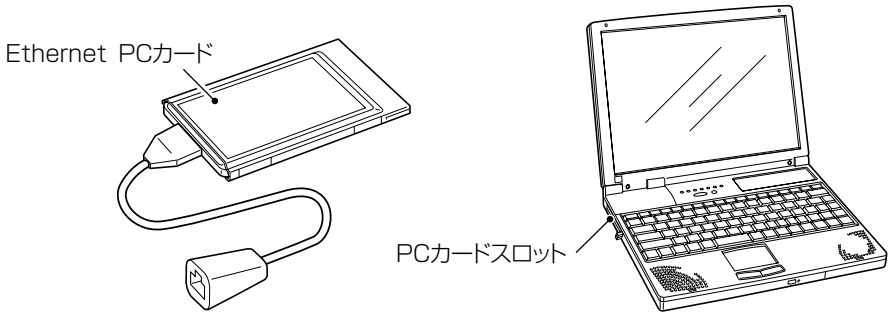
※出荷時や全設定初期化時、本製品のIPアドレスは、「192.168.0.1」、DHCPサーバー機能(☞P62、P69)は、「無効」に設定されています。
本製品の設定画面にアクセスするときは、接続するパソコンに固定IPアドレスの設定(☞P26～P29)が必要です。

有線LAN端末と接続して設定する場合

LANケーブルを接続できるパソコンをご用意ください。

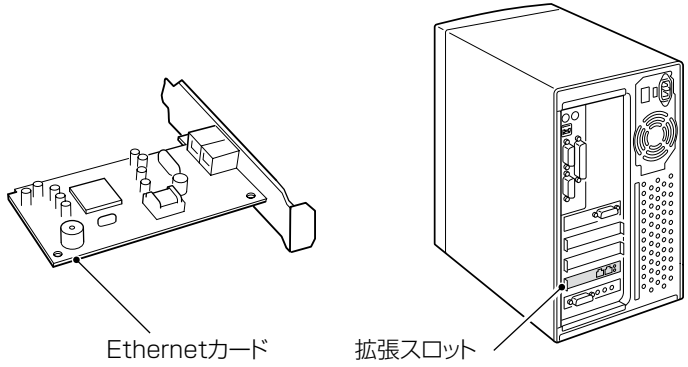
ノートブック型パソコンの場合

ご使用のパソコンに対応したEthernetカードを取り付けてください。



デスクトップ型パソコンの場合

拡張スロットには、PCIやISAなどの種類がありますので、ご使用のパソコンで空いているスロットをお調べになってから、Ethernetカードを取り付けてください。



無線LAN端末と接続して設定する場合

無線LAN機能搭載のパソコンをご用意ください。
本製品は、[IEEE802.11n/a(W52/W53/W56)/b/g]規格に準拠しています。

※出荷時、本製品は、[IEEE802.11n/b/g]規格の無線LAN端末と通信します。

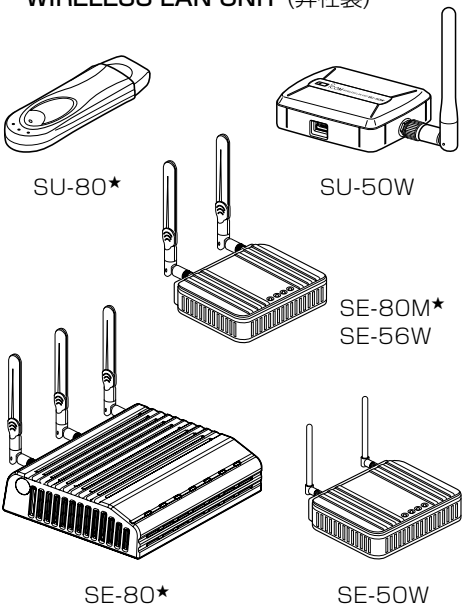
無線LAN機能を搭載しないパソコンをご使用の場合　　(2009年11月現在)

★印の製品は、[IEEE802.11n]規格に準拠、WPS機能に対応しています。

◎[USB]ポートを装備するパソコンには、右図のような弊社製WIRELESS LAN UNIT(SU-80★、SU-50W)をご用意しています。

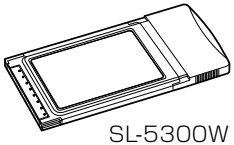
◎[LAN]ポートを装備するパソコンには、右図のような弊社製WIRELESS LAN UNIT(SE-80M★、SE-80★、SE-56W、SE-50W)をご用意しています。

WIRELESS LAN UNIT (弊社製)



◎[PCカードスロット]を装備するパソコンには、右図のような弊社製無線LANカード(SL-5300W)をご用意しています。

無線LANカード (弊社製)



※すでにお使いの弊社製無線LAN製品との対応については、本書177ページをご覧ください。

Step2. 固定IPアドレスを設定する

本製品の設定に使用するパソコンに固定IPアドレスを設定する手順について、Windows VistaとWindows XPを例に説明します。　（設定例：192.168.0.10）

※出荷時や全設定初期化時、本製品のIPアドレスは「192.168.0.1」、DHCPサーバー機能（☞P62、P69）は「無効」に設定されています。

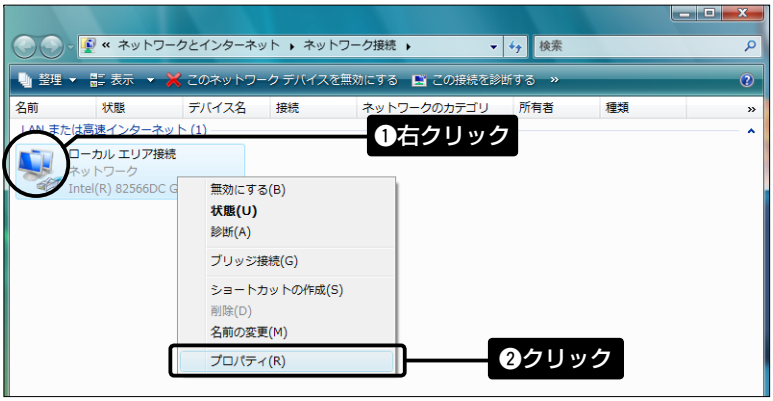
Windows Vistaの場合

1 マウスを〈スタート〉（ロゴボタン）→［コントロールパネル］の順に操作します。

2 コントロールパネルから、［ネットワークとインターネット］をクリックし、表示された画面で［ネットワークと共有センター］をクリックします。

3 タスク欄の［ネットワーク接続の管理］をクリックします。

4 ［ローカルエリア接続（有線LAN端末で設定する場合）］、または［ワイヤレスネットワーク接続（無線LAN端末で設定する場合）］を右クリックし、表示されたメニューから、［プロパティ（R）］をクリックします。

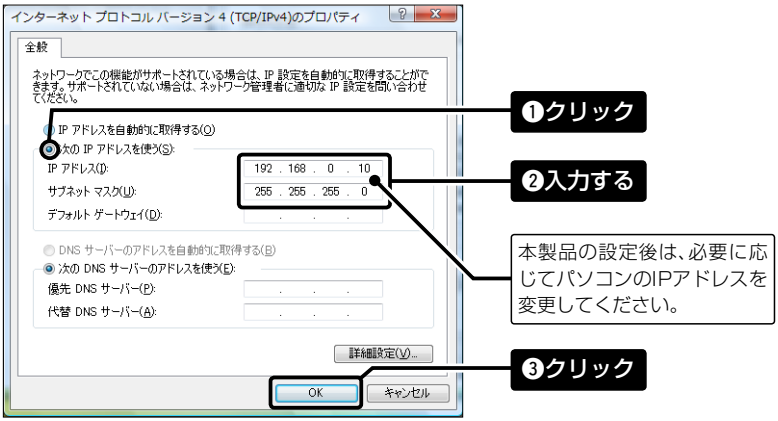


5 [ユーザーアカウント制御]のメッセージが表示された場合は、[続行]をクリックします。

6 「ローカル エリア接続のプロパティ」画面で、[インターネットプロトコル バージョン4(TCP/IPv4)]を選択し、〈プロパティ(R)〉をクリックします。

「インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティ」画面(別画面)を表示します。

7 [次のIPアドレスを使う(S)]をクリックし、[IPアドレス(I)](例:192.168.0.10)と[サブネットマスク(U)](例:255.255.255.0)を入力して、〈OK〉をクリックします。



※上図は、設定例です。

8 「ローカル エリア接続のプロパティ」画面で、〈閉じる〉をクリックします。

次ページにつづく➔

Step2. 固定IPアドレスを設定する

Windows XP場合

1 マウスを〈スタート〉→[コントロールパネル(C)]の順に操作します。

2 [ネットワークとインターネット接続]をクリックします。

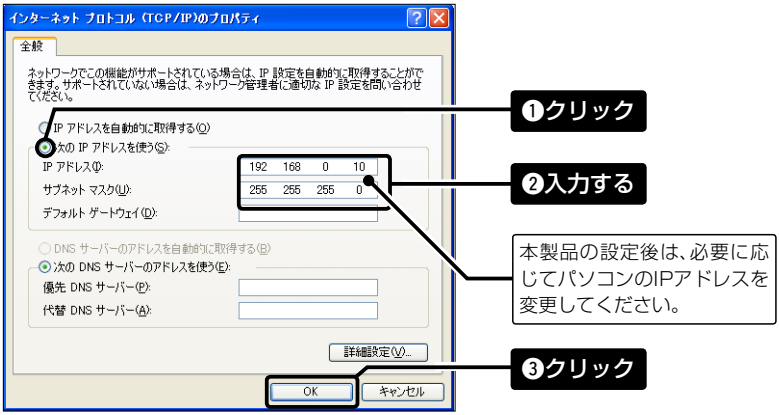
3 [ネットワーク接続]アイコンをクリックします。

4 [ローカルエリア接続](または、[ワイヤレスネットワーク接続])アイコンを右クリックすると表示されるメニューから、[プロパティ(R)]をクリックします。

5 「ローカル エリア接続のプロパティ」画面の[全般]タブで、「インターネット プロトコル(TCP/IP)」を選択し、〈プロパティ(R)〉をクリックします。

「インターネット プロトコル(TCP/IP)のプロパティ」画面(別画面)を表示します。

6 [次のIPアドレスを使う(S)]をクリックし、[IPアドレス(I)]と[サブネットマスク(U)]を入力して、〈OK〉をクリックします。



※上図は、設定例です。

7 「ローカル エリア接続のプロパティ」画面で、〈閉じる〉をクリックします。

Step3. 設定に使うパソコンの接続

本製品に接続するHUBと既存のネットワークは、切りはなして設定してください。

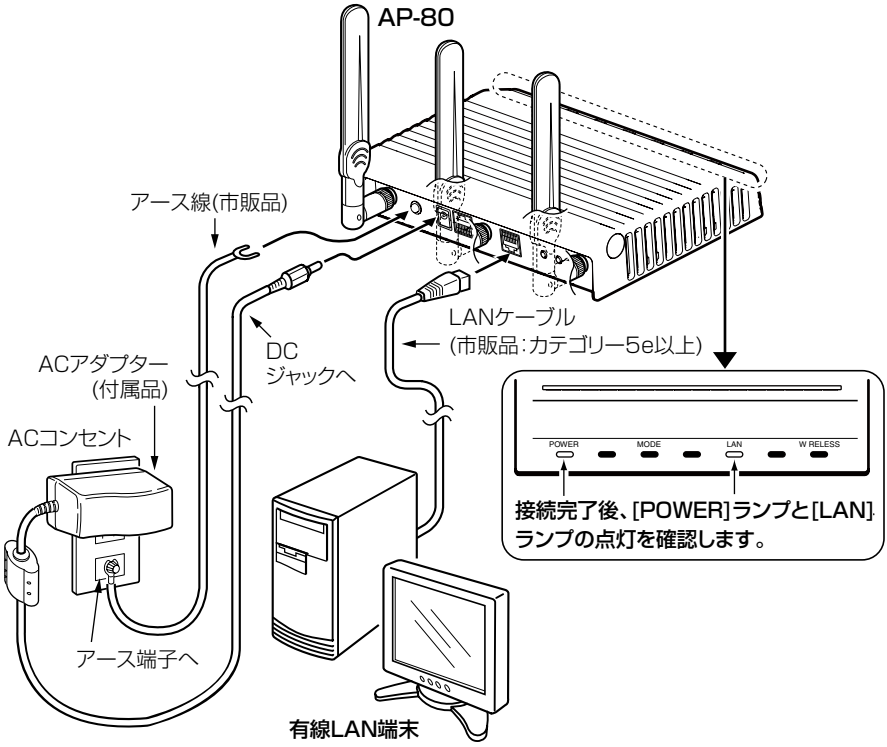
※本製品の[LAN]ポートは、MDI(ストレート)/MDI-X(クロス)の自動判別機能に対応しています。
HUBをお持ちでない場合でも、ストレート結線されたLANケーブルで本製品とパソコンを直接接続できます。

※HUBが802.3afに対応している場合は、付属のACアダプターを接続する必要はありません。

有線LAN端末を使用する場合

【ご注意】 接続するときは、本製品および接続する機器の電源を切ってください。

本製品とパソコン(有線LAN端末)の電源を入れます。



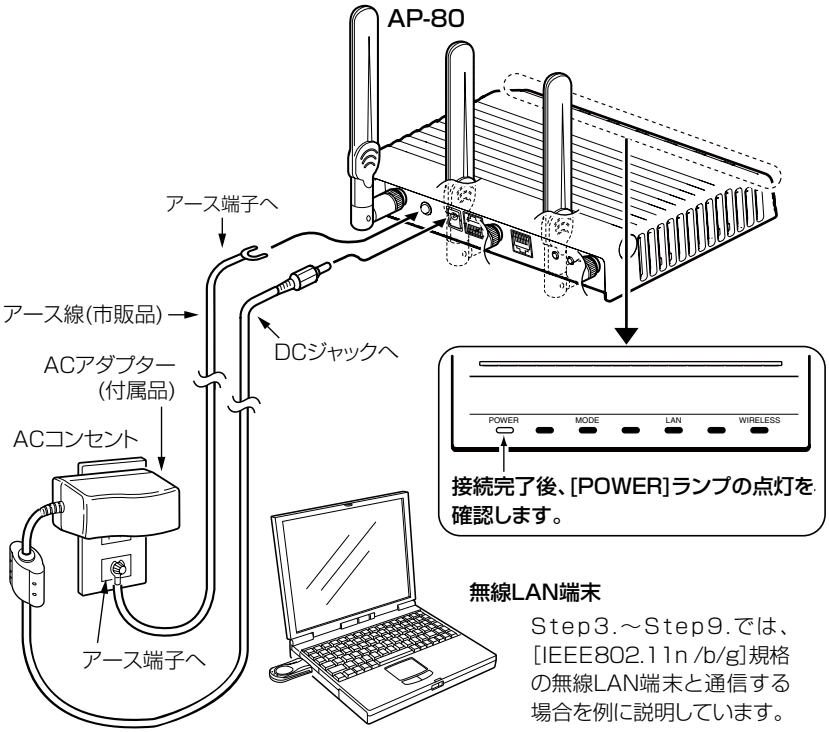
⚠警告 本製品のアース端子は、市販のアース線を使用して、コンセントのアース端子、または地中に埋めたアース棒(市販品)に必ず接続してください。
※落雷したときの電気的ショックの緩和、感電やノイズの回り込みを防止できます。
※絶対に、ガス管や水道管には接続しないでください。

無線LAN端末(Windows Vista)を使用する場合

Windows XPを使用する場合は、本書34ページをご覧ください。

【ご注意】 接続するときは、本製品および接続する機器の電源を切ってください。

1 本製品の電源を入れ、無線LANに対応するパソコン(無線LAN端末)の電源を入れます。



無線LAN端末

Step3.～Step9.では、[IEEE802.11n /b/g]規格の無線LAN端末と通信する場合を例に説明しています。

⚠警告 本製品のアース端子は、市販のアース線を使用して、コンセントのアース端子、または地中に埋めたアース棒(市販品)に必ず接続してください。
※落雷したときの電気的ショックの緩和、感電やノイズの回り込みを防止できます。
※絶対に、ガス管や水道管には接続しないでください。

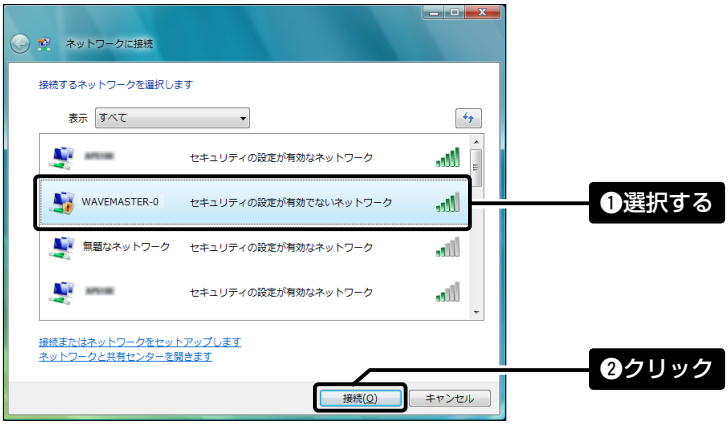
次ページにつづく➔

Step3. 設定に使うパソコンの接続

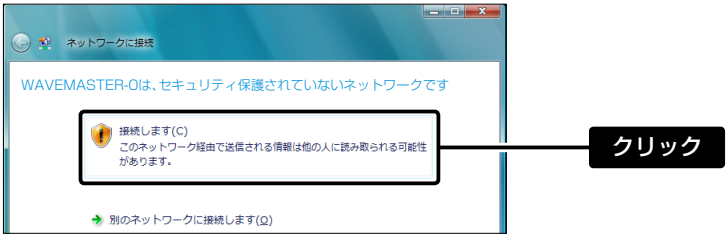
無線LAN端末(Windows Vista)を使用する場合

2 下記のような内容を画面に表示する場合は、[ネットワーク]アイコンをクリックします。(環境により、下記が表示されるまで数分かかることがあります。)

3 本製品に設定された[SSID](出荷時の設定:WAVEMASTER-0)を選択し、〈接続(O)〉をクリックします。



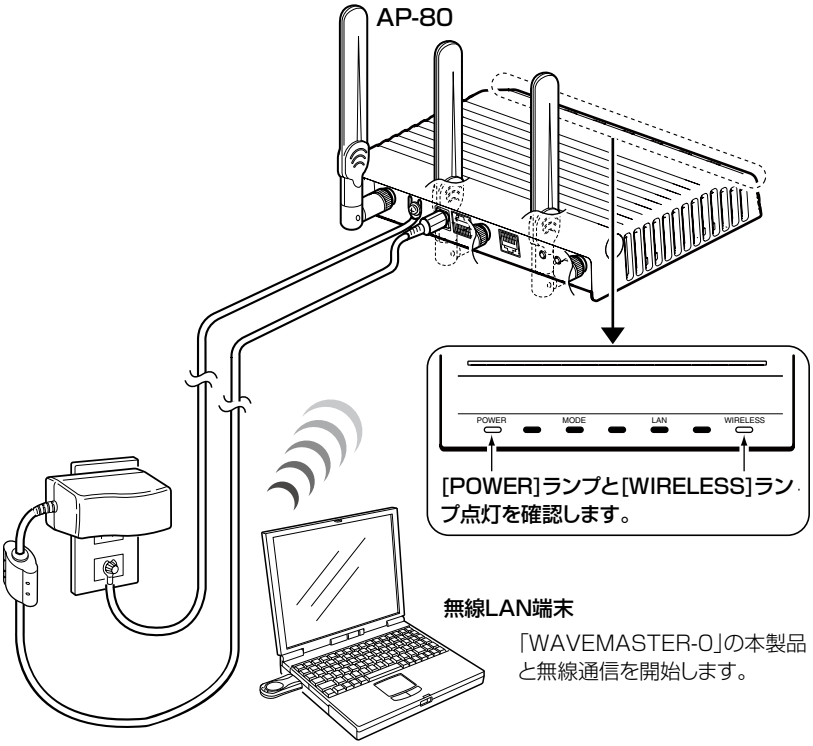
4 表示された画面の〈接続します(C)〉をクリックします。



※ 本製品に暗号鍵(キー)を設定した場合は、「ネットワークキー」入力画面が表示されますので、画面にしたがって暗号鍵(キー)を入力してください。

5 「正しく接続しました」と表示されたことを確認します。

6 本製品の[WIRELESS]ランプが点灯したことを確認します。



次ページにつづく➔

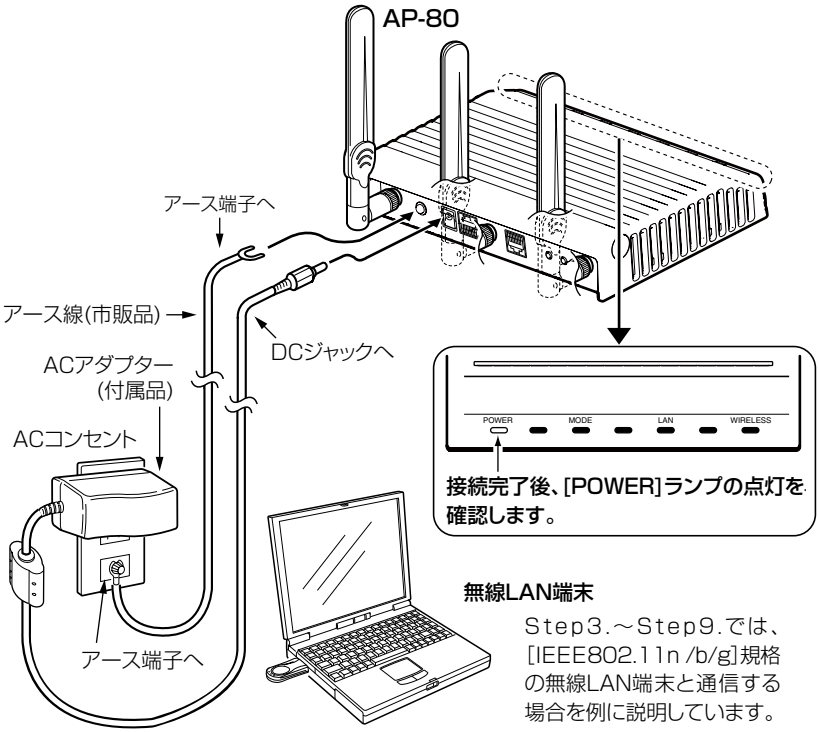
Step3. 設定に使うパソコンの接続

無線LAN端末(Windows XP)を使用する場合

Windows Vistaを使用する場合は、本書31ページをご覧ください。

【ご注意】 接続するときは、本製品および接続する機器の電源を切ってください。

1 本製品の電源を入れ、無線LANに対応するパソコン(無線LAN端末)の電源を入れます。



無線LAN端末

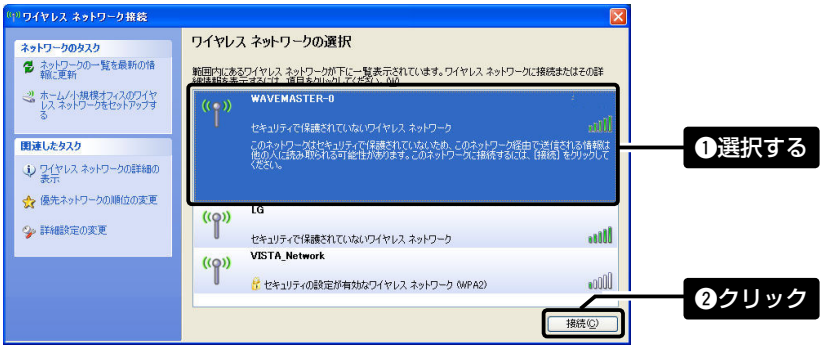
Step3.～Step9.では、[IEEE802.11n /b/g]規格の無線LAN端末と通信する場合を例に説明しています。

⚠警告 本製品のアース端子は、市販のアース線を使用して、コンセントのアース端子、または地中に埋めたアース棒(市販品)に必ず接続してください。
※落雷したときの電気的ショックの緩和、感電やノイズの回り込みを防止できます。
※絶対に、ガス管や水道管には接続しないでください。

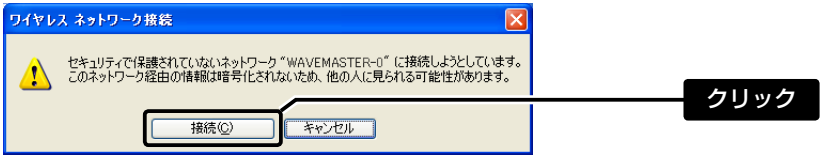
2 下記のような内容を画面に表示する場合は、[ワイヤレス ネットワーク接続]アイコンをクリックします。

※環境により、下記が表示されるまで数分かかることがあります。

3 本製品に設定された[SSID](出荷時の設定:WAVEMASTER-0)を選択し、〈接続(C)〉をクリックします。



4 表示された画面の〈接続(C)〉をクリックします。



※ 本製品に暗号鍵(キー)を設定した場合は、「ネットワークキー」入力画面が表示されますので、画面にしたがって暗号鍵(キー)を入力してください。

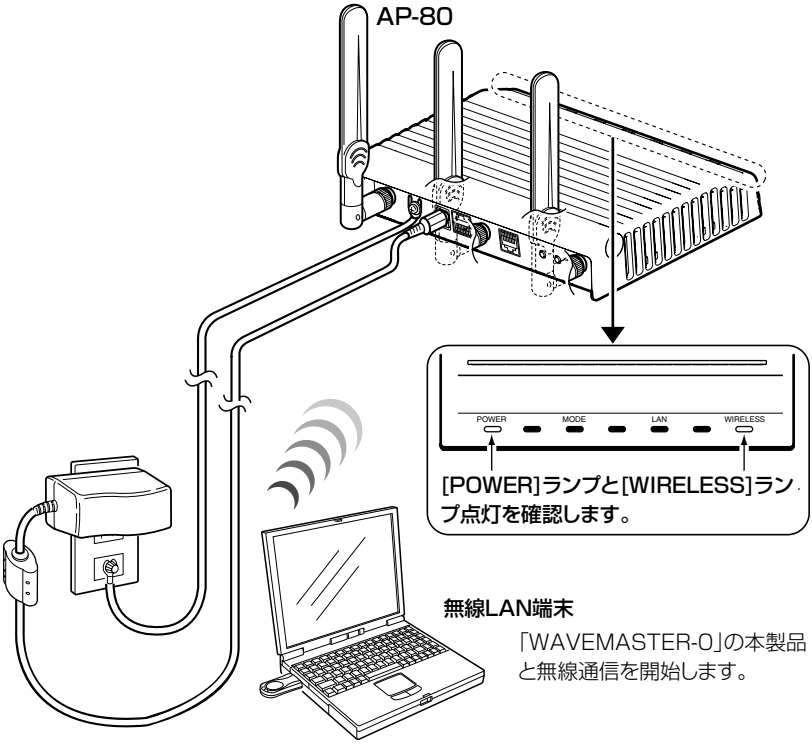
次ページにつづく➔

Step3. 設定に使うパソコンの接続

無線LAN端末（Windows XP）を使用する場合

5 「接続」と表示されたことを確認します。

6 本製品の[WIRELESS]ランプが点灯したことを確認します。



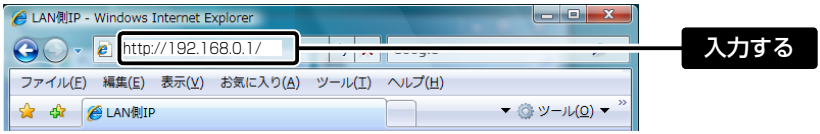
Step4. 設定画面へのアクセスを確認する

本製品に接続したパソコンのWWWブラウザーから、本製品を設定する画面にアクセスする手順について説明します。

設定画面にアクセスするには

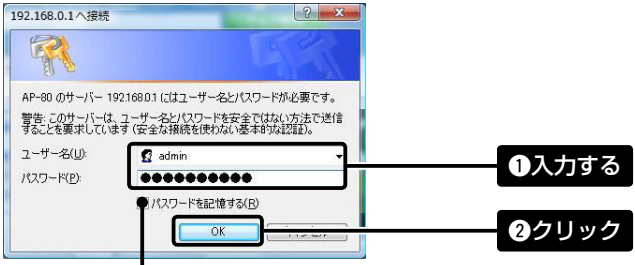
1 WWWブラウザーを起動します。

2 本製品に設定されたIPアドレスをWWWブラウザーのアドレスバーに入力します。
出荷時、本製品のIPアドレスは「192.168.0.1」に設定されています。



3 [Enter]キーを押します。
[ユーザー名(U):]と[パスワード(P):]を求める画面が表示されます。

4 [ユーザー名(U):]欄に「admin」、[パスワード(P):]欄に「wavemaster」(出荷時の設定)を入力し、〈OK〉をクリックすると、本製品の設定画面が表示されます。



クリックすると、パスワードが保存されます。
内容に変更がない場合は、次回のアクセスでは、〈OK〉をクリックするだけになります。

WWWブラウザーについて

ご使用になるWWWブラウザーは、Microsoft Internet Explorer6.0以降をご用意ください。
また、設定画面が正しく表示できるように、WWWブラウザーのJavaScript機能、およびCookieは有効にしてください。
本書では、Internet Explorer7.0を使用して説明しています。

Step5. 本体IPアドレスを変更する

本製品のIPアドレスを変更する手順について説明します。

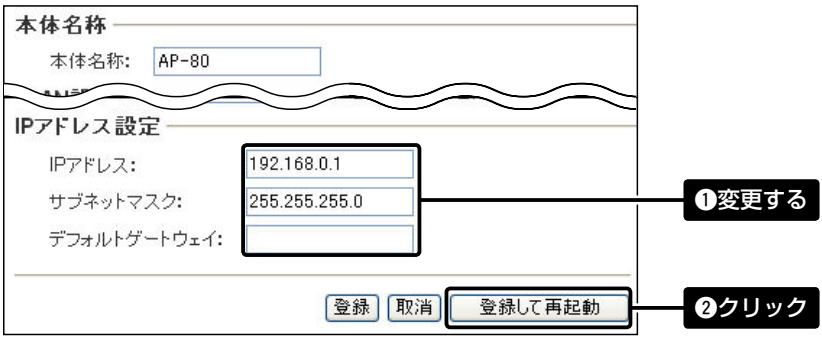
設定のしかた

「ネットワーク設定」→「LAN側IP」

既存のネットワークと重複しないように設定します。

1 「LAN側IP」画面で、[IPアドレス設定]項目の設定を変更し、〈登録して再起動〉をクリックします。

設定した内容が有効になります。



※IPアドレスの「ネットワーク部(例:192.168.0.)」を変更したときは、設定に使用するパソコン「ネットワーク部」についても本製品と同じに変更します。

2 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

[ユーザー名(U):]と[パスワード(P):]を求める画面が表示されます。(☞P37)

★WPS機能で、無線ネットワーク名(Step6.)と暗号化(Step7.)を自動設定する場合は、Step8.(☞P41)に進みます。

IPアドレスの割り当てかた

IPアドレスは、「ネットワーク部」と「ホスト部」の2つの要素から成り立っています。
出荷時の本製品のIPアドレス「192.168.0.1」(クラスC)を例とすると、最初の「192.168.0.」までが「ネットワーク部」で、残りの「1」を「ホスト部」といいます。
「ネットワーク部」が同じIPアドレスを持つネットワーク機器(パソコンなど)は、同じネットワーク上にあると認識されます。
さらに「ホスト部」によって同じネットワーク上にある各ネットワーク機器を識別しています。
以上のことから、IPアドレスを割り当てるときは、次のことに注意してください。

- 同じネットワークに含めたいネットワーク機器に対しては、「ネットワーク部」をすべて同じにする
- 同じネットワーク上の機器に対して、「ホスト部」を重複させない
- ネットワークアドレス(ホスト部の先頭および「0」)を割り当てない
- ブロードキャストアドレス(ホスト部の末尾および「255」)を割り当てない

Step6. 無線ネットワーク名を設定する

無線LAN端末との識別に必要なSSIDやANY接続による不正アクセス防止を設定します。
※[IEEE802.11n/b/g]規格の無線LAN端末と通信する場合を例に説明しています。

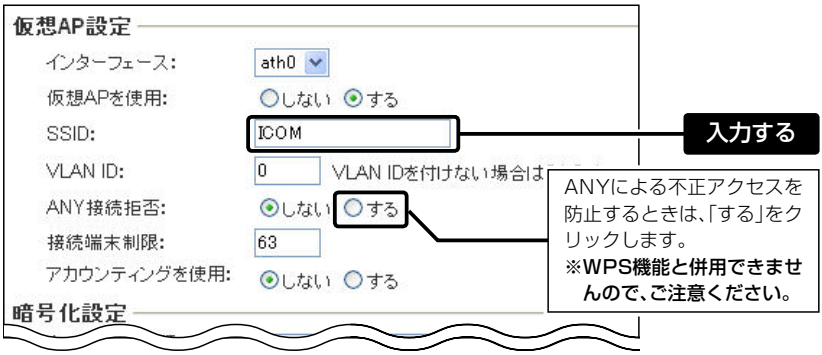
設定のしかた

「無線設定」→**「仮想AP」**

- SSID　　:任意に変更します。(出荷時の設定:WAVEMASTER-0)
- ANY接続拒否　:[SSID]を「ANY」に設定する無線LAN端末のアクセスを禁止します。

1 「無線設定」メニュー、「仮想AP」の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

2 [仮想AP設定]項目の[SSID:]欄に、大文字/小文字の区別に注意して、任意の半角英数字32文字以内で入力します。　(入力例:ICOM)



3 Step7.で暗号化を設定しますので、ここでは〈登録〉をクリックします。
「再起動が必要な項目が変更されています。」が表示されます。
※再起動するまで変更した設定内容は有効になりません。

「ANY」での不正アクセスについて

暗号化の設定をしないで無線LAN端末をご使用の場合、無線LAN端末側がANY接続を許可するように設定されていると、本製品の[SSID]の設定に関係なくこの無線LAN端末から本製品にアクセスを許可します。
アクセスを許可しない場合は、上記画面で[ANY接続拒否]の設定を「する」に変更すると、本製品の[SSID]をWindows XP、Windows Vista標準のワイヤレスネットワーク接続画面に表示させないようにできます。

Step7. 暗号化を設定する

無線LANで送受信するデータを暗号化する設定です。
※[IEEE802.11n/b/g]規格の無線LAN端末と通信する場合を例に説明しています。

設定のしかた

「無線設定」→「仮想AP」

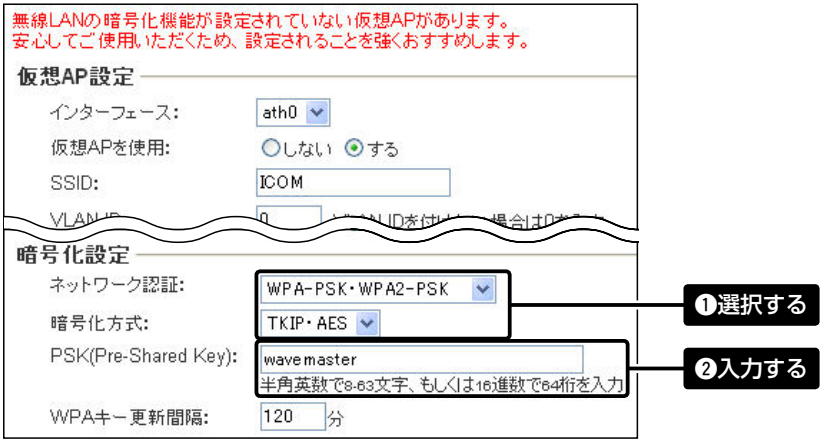
通信する相手の無線LAN端末にも同じ設定をしてください。

設定例）
- ネットワーク認証　:「WPA-PSK ·WPA2-PSK」
- 暗号化方式　:「TKIP ·AES」
- PSK(Pre-Shared Key)　:「wavemaster」

※設定例以外の暗号化設定については、本書47ページ～51ページをご覧ください。

1 [ネットワーク認証:]欄を「WPA-PSK ·WPA2-PSK」に選択し、選択したとき表示された[暗号化方式:]欄で「TKIP ·AES」を選択、[PSK(Pre-Shared Key):]欄で「wavemaster」と半角で入力します。

※[PSK(Pre-Shared Key):]欄に入力した文字数によって、入力モード(ASCII:半角で8～63文字入力/16進数:64桁入力)を自動判別します。



2 〈登録して再起動〉をクリックします。

3 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

Step8. WPS機能を有効にする

無線ネットワーク名(Step6.)と暗号化(Step7.)を自動設定するために、WPS(Wi-Fi Protected Setup)機能を使用できるように設定します。
※[IEEE802.11n/b/g]規格の無線LAN端末と通信する場合を例に説明しています。

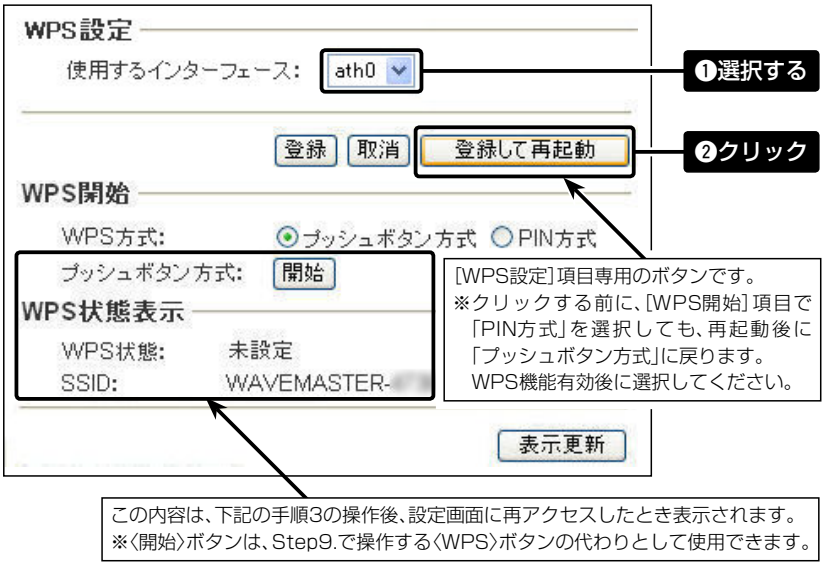
設定のしかた

「無線設定」→「WPS」

「プッシュボタン方式」(☞P139、P140)を例に説明します。
※WPS機能を有効にすると、本製品の後面パネルにある〈WPS〉ボタンの操作が有効になります。
なお、無線ネットワーク名(Step6.)と暗号化(Step7.)で設定している内容は、無効になります。

1 「無線設定」メニュー、「WPS」の順にクリックします。
「WPS」画面を表示します。

2 WPS機能を使用する仮想APを[使用するインターフェース:]欄で選択(例:ath0)して、〈登録して再起動〉の順にクリックします。



3 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

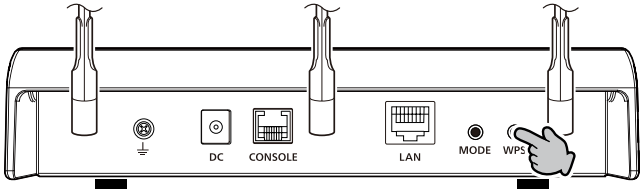
Step9.〈WPS〉ボタンで自動設定を開始する

〈WPS〉ボタンを使用した自動設定の操作手順について説明します。
本製品で自動生成されたSSIDと共有鍵(キー)の内容を無線LAN端末に自動設定します。

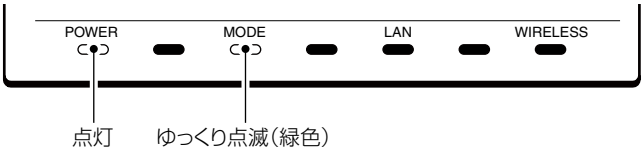
操作のしかた

無線LAN端末は、WPS対応のものをご用意ください。
JUMPSTART™アプリケーション(SU-80〈弊社製〉に付属)の操作を例に説明します。
※JUMPSTART™アプリケーションのインストールや詳細な使用方法については、パソコンに装着したWPS対応無線LAN製品に付属の取扱説明書をご覧ください。
※設定できない場合は、[使用するインターフェース]欄の設定(Step8.)を「なし」に戻してから、手動で設定(Step6.とStep7.)してください。

1 本製品の〈WPS〉ボタンを押します。
※指で押せないときは、ペン先などを利用してください。

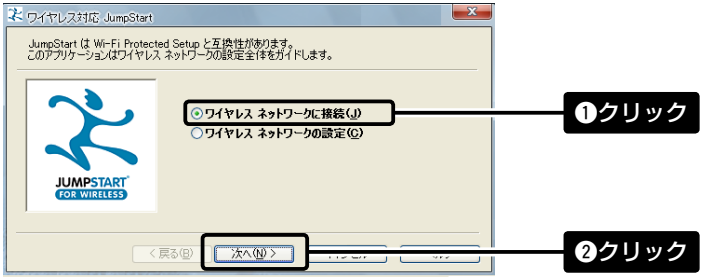


2 [MODE]ランプがゆっくり点滅(緑色)していることを確認します。
※無線LAN端末側の操作は、本製品の操作から2分以内に開始してください。
設定に失敗(2分以上経過)すると、[MODE]ランプの点滅が赤色(20秒後消灯)に切り替わりますので、はじめから操作をやりなおしてください。
※[LAN]ランプと[WIRELESS]ランプは、本製品の接続状態により異なります。

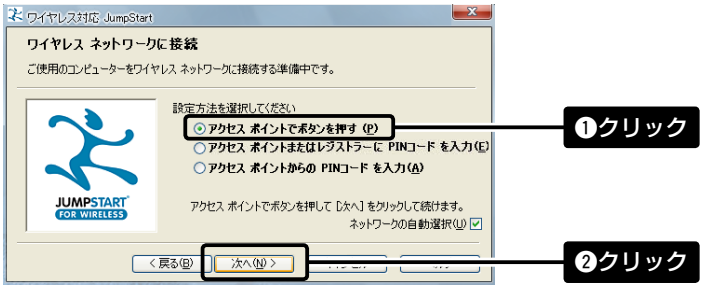


3 WPS対応無線LAN製品が装着された無線LAN端末から、JUMPSTART™アプリケーションを起動します。
※[IEEE802.11n/b/g]規格の無線LAN端末と通信する場合を例に説明しています。

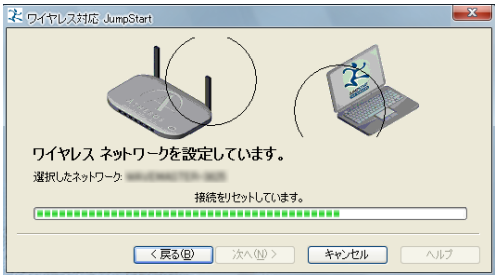
4 「ワイヤレスネットワークに接続(J)」、〈次へ(N)>〉の順にクリックします。



5 「アクセスポイントでボタンを押す(P)」、〈次へ(N)>〉の順にクリックします。



6 自動設定を開始すると、下記の画面を表示します。
次の画面に切り替わるまで、しばらく待ちます。

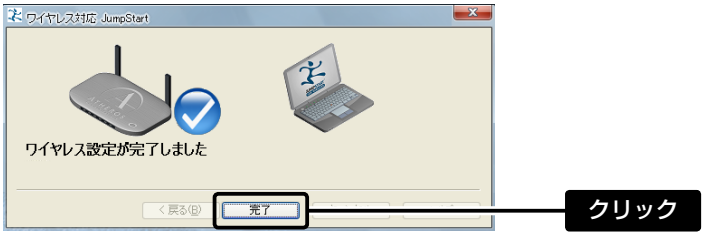


次ページにつづく➔

Step9.〈WPS〉ボタンで自動設定を開始する

操作のしかた

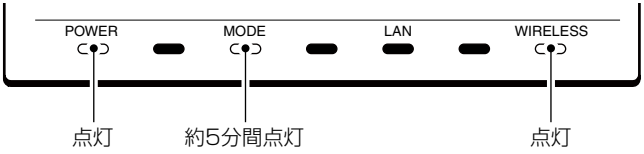
7 下記の画面が表示されたら、〈完了〉をクリックします。



※「ワイヤレス設定が完了しました」と表示された下に、上記以外の内容を表示する場合は、自動設定に失敗していますので、はじめからやりなおしてください。

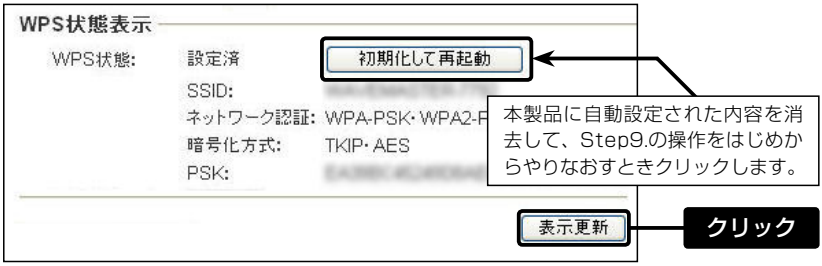
8 本製品の[MODE]ランプと[WIRELESS]ランプが点灯します。

※約5分後、[MODE]ランプは、消灯します。
※[LAN]ランプは、本製品の接続状態により異なります。



9 〈表示更新〉をクリックします。

本製品に自動設定された内容を表示します。
※下記の設定内容を2台目以降の無線LAN端末に自動設定するときは、別の無線LAN端末を使用して、Step9.の手順1.から操作してください。



無線LANの詳細設定

第3章

この章では、
無線LANの詳細な機能を設定する手順について説明します。

1. [IEEE802.11n/a]規格で無線通信するには …… 46
2. [WEP RC4]暗号化を設定するには …… 47
   暗号鍵(キー)の入力について …… 47
   ASCII文字→16進数変換表について …… 47
   16進数で暗号鍵(キー)を入力するには …… 48
   ASCII文字で暗号鍵(キー)を入力するには …… 49
   暗号鍵(キー)を生成するには …… 50
   暗号鍵(キー)値の設定例 …… 51
3. 自動設定したいSSIDと共有鍵(キー)を指定するには …… 52
4. 仮想APを設定するには …… 56
5. MACアドレスフィルタリングを設定するには …… 58

1. [IEEE802.11n/a]規格で無線通信するには

[IEEE802.11n/a(W52/W53/W56)]規格の無線LANカードを装着するパソコンを使用して、本製品と無線通信するには、次の手順で変更してください。

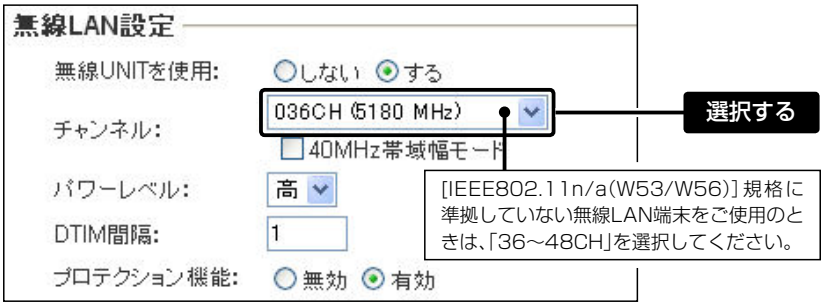
設定のしかた

「無線設定」→**「無線LAN」**

出荷時や全設定初期化時、チャンネルは「001CH(2412MHz)」に設定されています。

1 「無線設定」メニューをクリックします。
「無線LAN」画面を表示します。

2 チャンネルを選択します。



3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

DFS機能について

[IEEE802.11n/a(W53/W56)]規格のチャンネル(☞P3)を設定すると有効になります。
本製品の再起動後や電源投入直後の約1分間は、気象レーダーなどの電波検出を開始すると同時に、本製品へのアクセスをすべて停止して、[WIRELESS]ランプが約1分間点滅します。
[IEEE802.11n/a(W53)]規格のチャンネルは、干渉しない[IEEE802.11n/a(W52/W53)]規格のチャンネルに自動で変更され、[IEEE802.11n/a(W52)]規格のチャンネルに変更されたときは、DFS機能を停止します。
[IEEE802.11n/a(W56)]規格のチャンネルは、同じ規格で干渉しない別のチャンネルに変更されます。

2. [WEP RC4]暗号化を設定するには

[WEP RC4]暗号化を設定する仮想の暗号鍵(キー)による設定は、次のとおりです。

- 16進数で暗号鍵(キー)を直接入力する(☞P48)
- ASCII文字で暗号鍵(キー)を直接入力する(☞P49)
- [キージェネレーター]に入力した文字列より暗号鍵(キー)を生成する(☞P50)

※ [WEP RC4]暗号化を設定できないときは、使用する仮想AP(ath0～ath3)にWPS機能(☞P41)が設定されていないことを確認してください。

※ [WPA-PSK(TKIP)/(AES)]暗号化設定例については、本書40ページをご覧ください。

暗号鍵(キー)の入力について

[暗号化方式]の設定によって、入力する暗号鍵(キー)の文字数や桁数が異なります。
また、入力された文字数、および桁数によって、入力モード(16進数/ASCII文字)を自動判別します。

ネットワーク認証	入力モード / 暗号化方式	16進数(HEX)	ASCII文字
オープンシステム/共有キー	WEP RC4 64(40)ビット	10桁	5文字(半角)
	WEP RC4 128(104)ビット	26桁	13文字(半角)
	WEP RC4 152(128)ビット	32桁	16文字(半角)

※入力できる桁数および文字数は、( )内のビット数に対する値です。

※無線LAN端末側で、[キーインデックス]の設定を「1」以外で使用している場合は、[キーインデックス]を「1」に変更して、そのテキストボックスに本製品と同じ暗号鍵(キー)を設定してください。(☞P51)

ASCII文字→16進数変換表について

相手が指定する[入力モード]で暗号鍵(キー)を設定できない場合は、下記の変換表を参考に指示された暗号鍵(キー)に対応する記号や英数字で入力してください。

[例]16進数入力で「4153434949」(10桁)を設定している場合、ASCII文字では、「ASCII」(5文字)になります。

ASCII文字		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
16進数		21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f
ASCII文字	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
16進数	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f
ASCII文字	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16進数	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f
ASCII文字	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
16進数	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f
ASCII文字	`	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o
16進数	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f
ASCII文字	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
16進数	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	

2. [WEP RC4]暗号化を設定するには

16進数で暗号鍵(キー)を入力するには

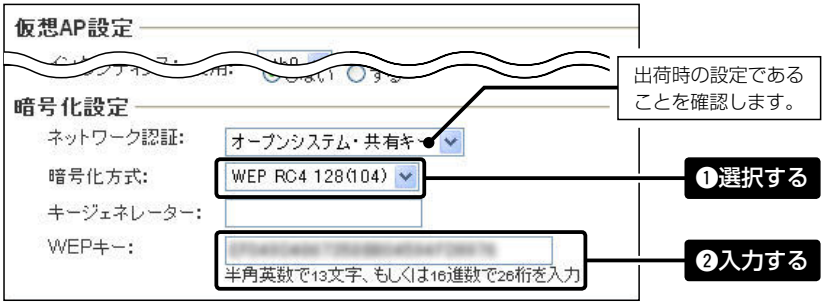
「無線設定」→「仮想AP」

出荷時や全設定初期化時、暗号化は設定されていません。
次の条件で設定する場合を例に説明します。

- [ネットワーク認証:]　:「オープンシステム・共有キー」(出荷時の設定)
- [暗号化方式:]　:「WEP RC4 128(104)」ビット
- [WEPキー:]　:「0～9」、および「a ～f(またはA ～F)」を使用して、26桁を入力

1 「無線設定」メニュー、[仮想AP]の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

2 [暗号化方式:]欄で「WEP RC4 128(104)」を選択し、26桁の暗号鍵(キー)を[WEPキー:]欄に入力します。



3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

無線LAN端末のキーインデックスについて(Windows XP Service Pack適用時を除く)
Service Packを適用していないWindows XP標準のワイヤレスネットワーク接続を使用して本製品と[WEP RC4]で通信する場合、無線LAN端末側のキーインデックスを「0」に設定してください。
キーインデックスが「1」～「3」に設定されているときは、本製品と通信できません。

ASCII文字で暗号鍵(キー)を入力するには

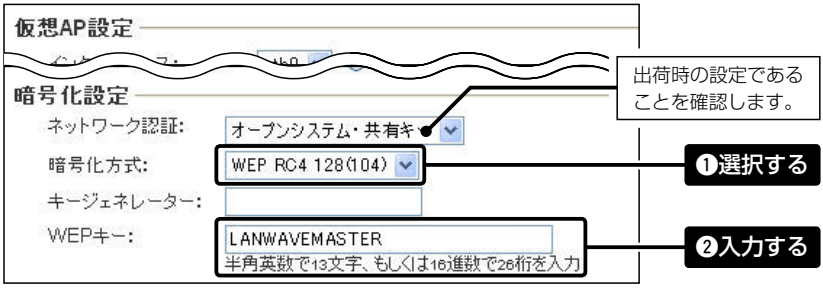
「無線設定」→「仮想AP」

出荷時や全設定初期化時、暗号化は設定されていません。
次の条件で設定する場合を例に説明します。

- [ネットワーク認証:]　:「オープンシステム・共有キー」(出荷時の設定)
- [暗号化方式:]　:「WEP RC4 128(104)」ビット
- [WEPキー:]　:13文字を入力(例:LANWAVEMASTER)

1 「無線設定」メニュー、[仮想AP]の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

2 [暗号化方式:]欄で「WEP RC4 128(104)」を選択し、13文字の暗号鍵(キー)を[WEPキー:]欄に入力します。



3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

2. [WEP RC4]暗号化を設定するには

暗号鍵(キー)を生成するには

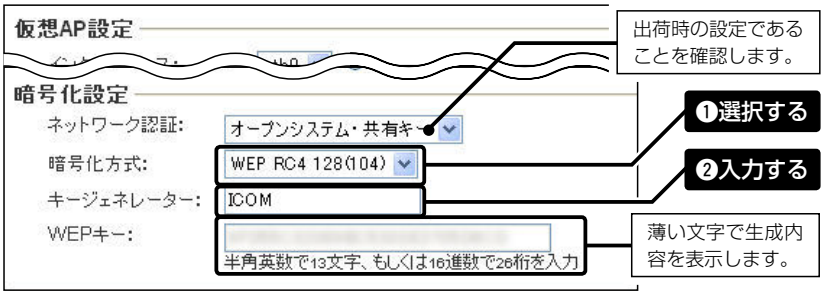
「無線設定」→**「仮想AP」**

出荷時や全設定初期化時、暗号化は設定されていません。
次の条件で設定する場合を例に説明します。

- [ネットワーク認証:]　:「オープンシステム・共有キー」(出荷時の設定)
- [暗号化方式:]　:「WEP RC4 128(104)」ビット
- [キージェネレーター:]　:任意の文字列(半角英数字31文字以内)を入力(例:ICOM)

1 「無線設定」メニュー、[仮想AP]の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

2 [暗号化方式:]欄で「WEP RC4 128(104)」を選択し、任意の文字列を[キージェネレーター:]欄に入力(例:ICOM)します。



3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

キージェネレーターについて

◎ 任意の文字列を入力すると、「16進数」の暗号鍵(キー)が[WEPキー:]欄のテキストボックスに自動生成されます。
◎ [WEPキー:]欄のテキストボックスに生成される桁数および文字数は、選択する[暗号化方式]によって異なります。
※キージェネレーターは、弊社以外の機器と互換性はありません。

暗号鍵(キー)値の設定例

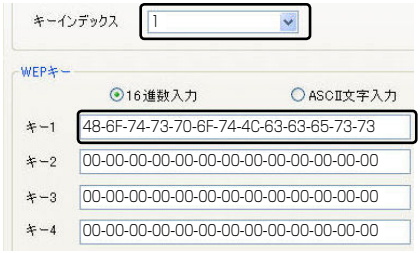
弊社製無線LANカードに付属の設定ユーティリティーで本製品に接続する場合は、下記の設定例を参考にしてください。

※「WEP RC4 128(104)」ビットの暗号化方式を使用して、「486F7473706F744C6363657373」(16進数(26桁)の暗号鍵(キー)で本製品と無線LAN端末の両方に直接入力する場合を例に説明します。本製品と無線LAN端末で暗号鍵(キー)値が異なる場合は、通信できません。

◎キーインデックス「1」のWEPキー(値)が本製品と同じため通信できます。

※キー1の暗号鍵(キー)がデータの送信と受信に使用されます。

AP-80側 ⇄ **弊社製無線LAN端末側(例:SU-80)**



キーインデックスについて

本製品には、キーインデックスの設定はありませんが、「1」に相当します。

※無線LAN端末側で、[キーインデックス]の設定を「1」以外で使用している場合は、[キーインデックス]を「1」に変更して、そのテキストボックスに本製品と同じ暗号鍵(キー)を設定してください。

3. 自動設定したいSSIDと共有鍵(キー)を指定するには

あらかじめ、SSIDと暗号化(WPA-PSK/WPA2-PSK)を本製品で使用する仮想APに設定し、その内容をWPS機能で、WPS機能対応無線LAN端末に自動設定する手順を説明します。

※[IEEE802.11n/b/g]規格の無線LAN端末に自動設定する場合を例に説明しています。

設定のしかた

「無線設定」→「WPS」

「プッシュボタン方式」(☞P139、P140)を例に説明します。

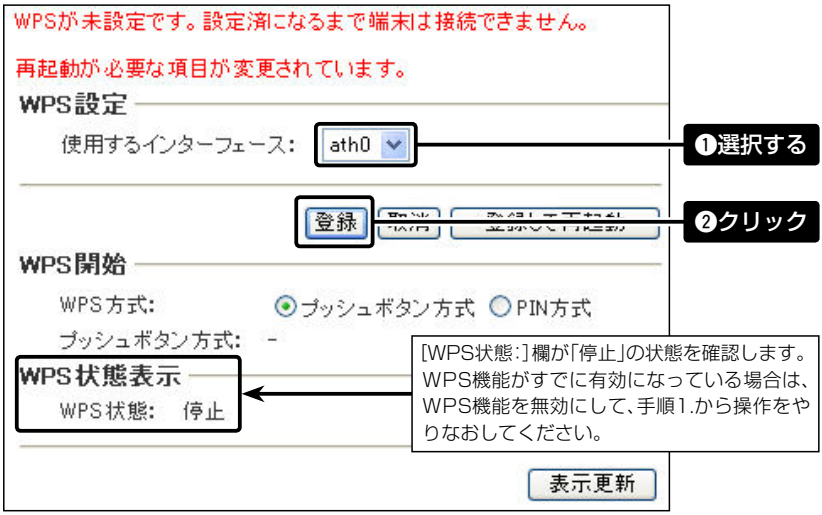
※ 自動設定する内容は、下記の操作で〈WPS〉ボタンの操作を有効にしたあと、「仮想AP」画面(〈例〉インターフェース:ath0)の[暗号化設定]項目で設定(☞P53)が必要です。

1 「無線設定」メニュー、「WPS」の順にクリックします。

「WPS」画面を表示します。

2 [使用するインターフェース:]欄で「ath0」を選択し、〈登録〉をクリックします。

「WPSが未設定です。設定済になるまで端末は接続できません。」、「再起動が必要な項目が変更されています。」が表示されます。



設定のしかた(つづき)　「無線設定」→「仮想AP」

設定例)
- SSID　:「ICOM」
- ANY接続拒否　:WPS機能と併用できないため、「しない」でご使用ください。
- ネットワーク認証　:「WPA-PSK」
- 暗号化方式　:「AES」
- PSK(Pre-Shared Key)　:「wavemaster」

3 「無線設定」メニュー、「仮想AP」の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

4 SSIDを[仮想AP設定]項目の[SSID:]欄に入力します。
次に、[ネットワーク認証:]欄を「WPA-PSK」に選択し、選択したとき表示された[暗号化方式:]欄で「AES」を選択、[PSK(Pre-Shared Key):]欄で「wavemaster」と半角で入力します。
※[PSK(Pre-Shared Key):]欄に入力した文字数によって、入力モード(ASCII:半角で8〜63文字入力/16進数:64桁入力)を自動判別します。

5 〈登録して再起動〉をクリックします。

6 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

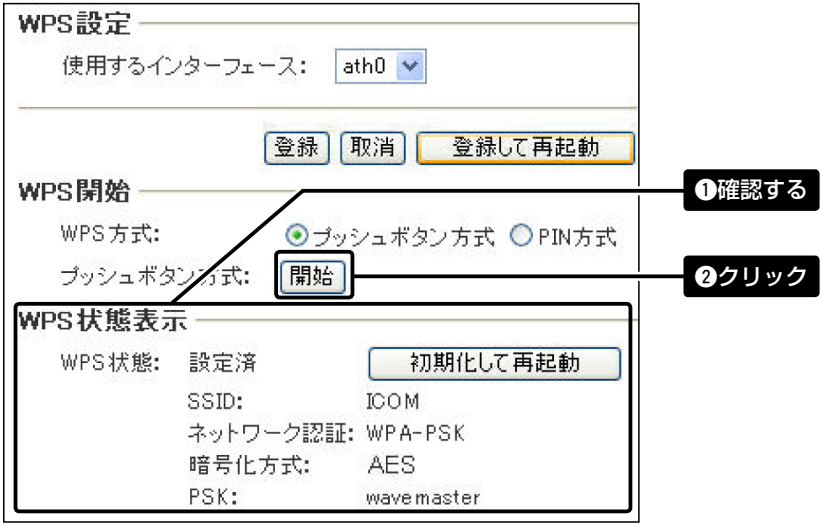
次ページにつづく➔

3. 自動設定したいSSIDと共有鍵(キー)を指定するには

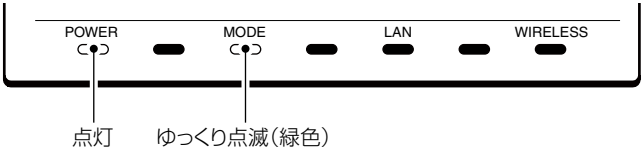
設定のしかた(つづき)　　「無線設定」→「WPS」

7 「無線設定」メニュー、「WPS」の順にクリックします。
「WPS」画面を表示します。

8 手順4.(☞P53)で設定した内容が下記の[WPS状態表示]項目に表示されていることを確認できたら、〈開始〉ボタン★をクリックします。
★本製品の後面パネルにある〈WPS〉ボタンを使用することもできます。



9 [MODE]ランプがゆっくり点滅(緑色)していることを確認します。
※無線LAN端末側の操作は、本製品の操作から2分以内に開始してください。
設定に失敗(2分以上経過)すると、[MODE]ランプの点滅が赤色(20秒後消灯)に切り替わりますので、はじめから操作をやりなおしてください。
※[LAN]ランプと[WIRELESS]ランプは、本製品の接続状態により異なります。



10 WPS対応無線LAN製品が装着された無線LAN端末から、JUMPSTART™アプリケーションを起動します。

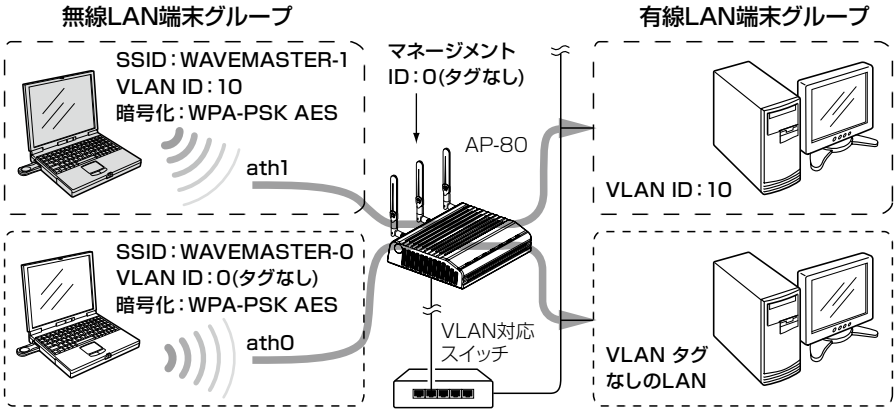
※ JUMPSTART™アプリケーションの操作については、本書43ページと同じですので、参考にしてください。

WPS対応
無線LAN端末

4. 仮想APを設定するには

下図の仮想AP無線VLANグループを構成するための設定手順を説明します。

※［SSID］を「WAVEMASTER-0」に設定する無線LAN端末グループは、設定されているものとします。



設定のしかた

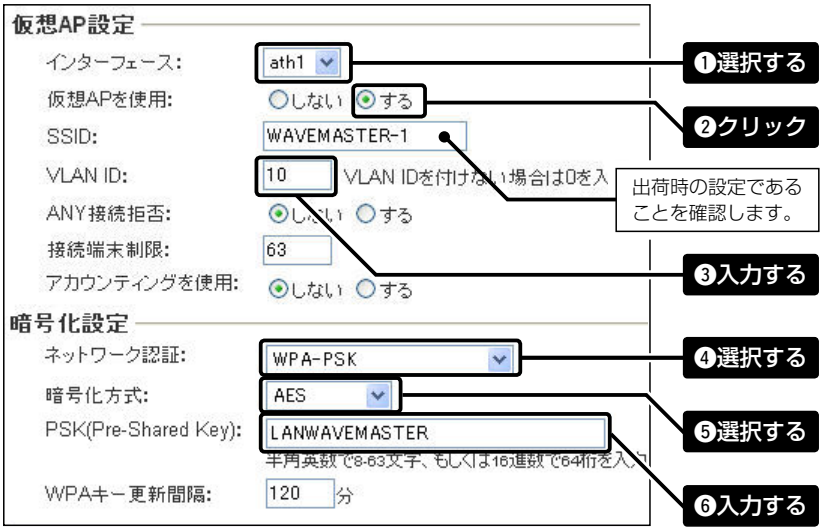
「無線設定」→「仮想AP」

上図の ■ 色で示す無線LAN端末について、次の条件を設定する例を説明します。
操作手順は、次ページで説明しています。

- ［仮想AP設定］項目　［インターフェース:］　:「ath1」
  ［仮想APを使用:］　:「する」
  ［SSID:］　:「WAVEMASTER-1」(出荷時の設定)
  ［VLAN ID:］　:「10」
- ［暗号化設定:］項目　［ネットワーク認証:］　:「WPA-PSK」
  ［暗号化方式:］　:「AES」
  ［PSK(Pre-Shared Key):］　:「LANWAVEMASTER」

1 「無線設定」メニュー、[仮想AP]の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

2 [インターフェース:]欄で「ath1」を選択し、前ページの設定条件にしたがって下記のように設定します。



3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

5. MACアドレスフィルタリングを設定するには

無線LAN端末のMACアドレスを登録する手順について説明します。
仮想AP(ath0～ath3)ごとに、異なる無線LAN端末を登録できます。

設定のしかた

「無線設定」→「MACアドレスフィルタリング」

本製品への接続を拒否する無線LAN端末の登録例を説明します。

1 「無線設定」メニュー、[MACアドレスフィルタリング]の順にクリックします。
「MACアドレスフィルタリング」画面(〈例〉インターフェース:ath0)を表示します。

2 [MACアドレスフィルタリングを使用:]欄で「する」、[フィルタリングポリシー:]欄で「拒否リスト」の順にクリックします。

3 〈登録〉をクリックします。
※〈登録して再起動〉をクリックした場合でも、本製品の再起動なしに設定内容が反映されます。

4 接続拒否として登録する無線LAN端末のMACアドレスを[MACアドレス:]欄に入力し、〈追加〉をクリックします。
入力したMACアドレスが[現在の登録]項目に表示されます。

※[現在の登録]項目の各欄についての説明は、本書123ページをご覧ください。

そのほかの基本設定

第 4 章

この章では、
そのほかに設定が必要と思われる機能について説明しています。

1. 設定画面へのアクセスを制限するには …… 60
2. 内部時計を設定するには …… 61
3. 本製品のDHCPサーバー機能を使用するには …… 62

1. 設定画面へのアクセスを制限するには

管理者用の[管理者パスワード]を設定することで、管理者以外がWWWブラウザーから本製品の設定を変更できないようにします。

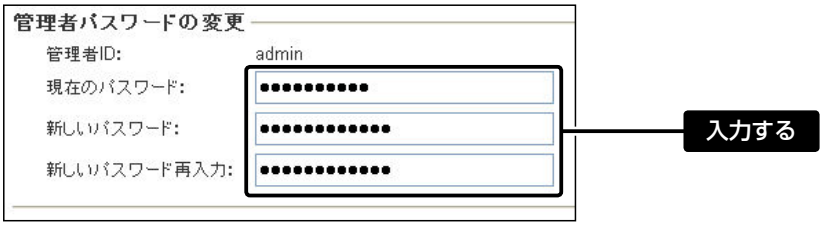
設定のしかた

「システム設定」→**「管理者」**

出荷時、本製品の設定画面には、[管理者ID(admin)]と[パスワード(wavemaster)]でアクセスできます。

1 「システム設定」メニューをクリックします。
「管理者」画面を表示します。

2 [現在のパスワード]欄、[新しいパスワード]欄、[新しいパスワード再入力]欄に、任意の英数字(半角31文字以内)で大文字/小文字の区別に注意して入力します。
入力した文字は、すべて「＊(アスタリスク)」、または「●(黒丸)」で表示されます。



3 〈登録〉をクリックします。
※〈登録して再起動〉をクリックした場合でも、本製品の再起動なしに設定内容が反映されます。

4 [ユーザー名(U)]と[パスワード(P)]を求める画面が表示されますので、設定した[管理者パスワード]を入力します。
本製品の設定画面を表示します。

【ご注意】
管理者パスワードを忘れた場合、設定を確認できなくなりますのでご注意ください。
※お忘れの場合、本製品の〈MODE〉ボタンを本書160ページの操作にしたがい、設定を工場出荷時(初期化)の状態に戻していただくことになります。

2. 内部時計を設定するには

本製品の内部時計を設定する手順について説明します。

※本製品の自動時計設定機能を使用する場合についても記載していますので、併せてご覧ください。

設定のしかた

「システム設定」→「時計」

本製品の内部時計を正確に表示させるため、設定されることをおすすめします。

1 「システム設定」メニュー、[時計]の順にクリックします。

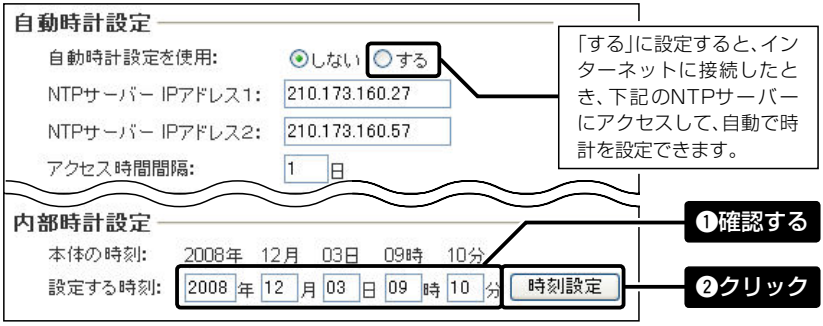
「時計」画面を表示します。

2 パソコンから自動取得した時刻が[内部時計設定]項目に表示されていることを確認し、〈時刻設定〉をクリックします。

内部時計に設定された時刻が、[本体の時刻]欄に表示されます。

※[設定する時刻]欄に表示されている時刻がパソコンと異なるときは、はじめからやりなおすと正確な時刻を取得できます。

※「時計」画面の〈登録〉では、時刻を設定できません。



※初期に参照しているNTPサーバーは、インターネットマルチフィード株式会社のものです。
http://www.jst.mfeed.ad.jp/

【ご注意】

本製品の電源を切ると、本製品の内部時計の設定が出荷時の状態に戻ります。
本製品の自動時計設定機能を使用しない場合は、停電や不慮の事故で電源が一時的に切れたときでも、内部時計の再設定が必要になります。
また、自動時計設定機能は、NTPサーバーへの問い合わせ先(経路)を設定する必要があります。
経路を設定しないときは、問い合わせできません。
「ネットワーク設定」メニュー→「LAN側IP」画面→[IPアドレス設定]項目にある[デフォルトゲートウェイ:]欄、または「ルーティング」画面の[スタティックルーティング設定]項目で、ルーティングテーブルを設定してください。

3. 本製品のDHCPサーバー機能を使用するには

有線LANおよび無線LANで本製品のDHCPサーバー機能を使用するときは、下記の手順でDHCPサーバー機能と自動割り当て開始IPアドレスを設定してください。

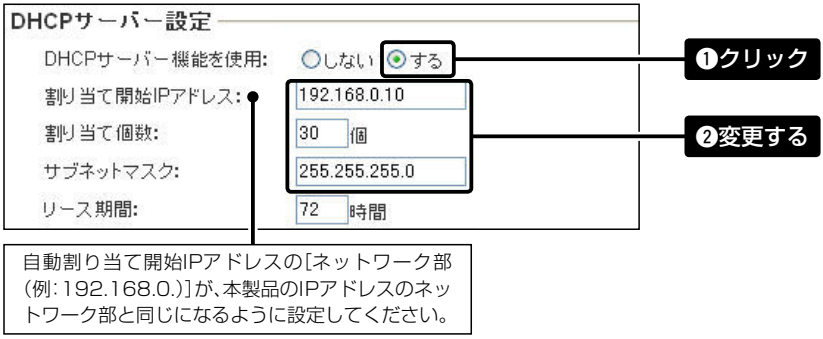
※本製品を接続するネットワーク上にDHCPサーバーが存在する場合に使用すると、IPアドレスの競合など、ネットワーク障害の原因になりますのでご注意ください。

設定のしかた

「ネットワーク設定」→「DHCPサーバー」

1 「ネットワーク設定」メニュー、[DHCPサーバー]の順にクリックします。
「DHCPサーバー」画面を表示します。

2 [DHCPサーバー設定]項目で、[DHCPサーバー機能を使用:]欄の「する」をクリックし、必要に応じて[割り当て開始IPアドレス]などを変更します。



3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 設定後、本製品のDHCPサーバーからIPアドレスを自動的に取得できるように、接続するパソコンのIPアドレス設定を変更し、設定画面にアクセスします。
[ユーザー名(U):]と[パスワード(P):]を求める画面が表示されます。

設定画面について

第5章

この章では、
各メニューで表示される設定画面について説明します。

1. 設定画面の名称と機能 …… 65
2.「LAN側IP」画面 …… 66
■ 本体名称 …… 66
■ VLAN設定 …… 66
■ IPアドレス設定 …… 67
3.「DHCPサーバー」画面 …… 69
■ DHCPサーバー設定 …… 69
■ 静的DHCPサーバー設定 …… 72
■ 現在の登録 …… 72
4.「ルーティング」画面 …… 73
■ IP経路情報 …… 73
■ スタティックルーティング設定 …… 74
■ 現在の登録 …… 74
5.「パケットフィルター」画面 …… 75
■ パケットフィルター …… 75
■ 現在の登録 …… 89
■ パケットフィルター使用例 …… 90
6.「無線LAN」画面 …… 96
■ 無線LAN設定 …… 96
7.「仮想AP」画面 …… 104
■ 仮想AP設定 …… 104
■ 暗号化設定 …… 108
8.「認証サーバー」画面 …… 118
■ RADIUS設定 …… 118
■ アカウンティング設定 …… 119
9.「MACアドレスフィルタリング」画面 …… 120
■ MACアドレスフィルタリング設定 …… 120
■ 端末MACアドレスリスト …… 122
■ 現在の登録 …… 123
■ 無線通信状態 …… 125

5 設定画面について

下記は、前ページからの「つづき」です。

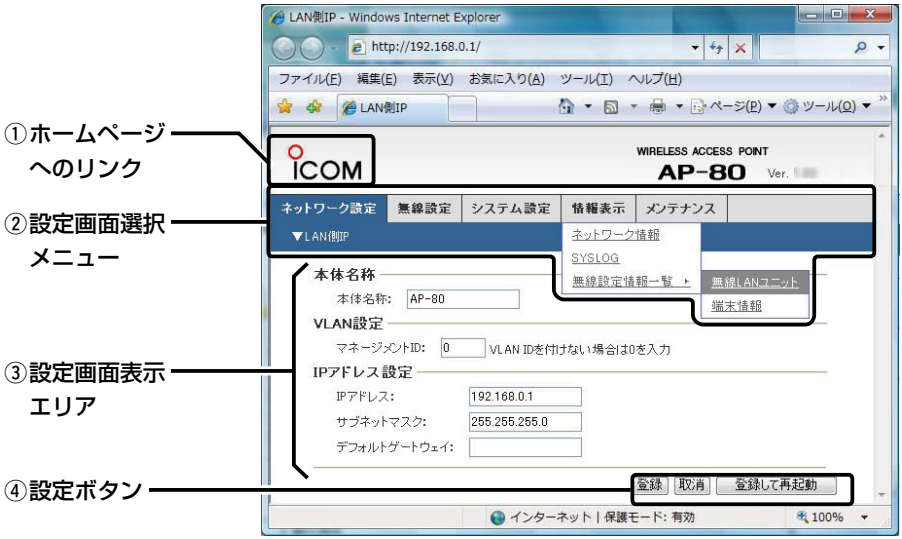
10.「WMM詳細」画面 …… 127
■ WMM詳細設定 …… 127
■ WMM共通設定 …… 132
11.「ARP代理応答」画面 …… 134
■ ARP代理応答 …… 134
■ ARPキャッシュ情報 …… 136
12.「WPS」画面 …… 137
■ WPS設定 …… 137
■ WPS開始 …… 139
■ WPS状態表示 …… 142
13.「管理者」画面 …… 143
■ 管理者パスワードの変更 …… 143
14.「時計」画面 …… 144
■ 自動時計設定 …… 144
■ 内部時計設定 …… 146
15.「SYSLOG」画面 …… 147
■ SYSLOG設定 …… 147
16.「SNMP」画面 …… 148
■ SNMP設定 …… 148
17.「ネットワーク情報」画面 …… 149
■ インターフェースリスト …… 149
■ 本体MACアドレス …… 149
■ 無線LANユニット …… 149
18.「SYSLOG」画面 …… 150
■ SYSLOG …… 150
19.「無線LANユニット」画面 …… 151
■ アクセスポイント情報 …… 151
■ 仮想AP一覧 …… 152
20.「端末情報」画面 …… 153
■ 端末情報 …… 153
■ 通信端末詳細情報 …… 154

【ご参考に】

設定画面は、各メニューとして用途ごとに分類されていますので、「設定画面の構成について」(☞P174～P175)と併せてご覧ください。
「メンテナンス」メニューについては、「保守について」(☞6章)で、操作方法と併せて説明しています。

1. 設定画面の名称と機能

本製品の設定画面の名称と各画面に含まれる項目を説明します。
設定画面の構成について詳しくは、本書174ページ～175ページをご覧ください。



①ホームページへのリンク

インターネットに接続できる環境で、アイコンをクリックすると、弊社のホームページを閲覧できます。

②設定画面選択メニュー

各メニューのタイトル上にマウスカーソルを合わせると、そのメニューに含まれる画面名称(例:ネットワーク情報/SYSLOG/無線設定情報一覧)を表示します。

※階層のあるメニューには、▶印が表示されています。

③設定画面表示エリア

[設定画面選択メニュー]で選択したメニューに含まれる画面名称(例:ネットワーク情報/SYSLOG)をクリックしたとき、その画面の内容を表示します。

④設定ボタン

設定した内容の登録や取り消しをします。〈登録〉をクリックして、「再起動が必要な項目が変更されています。」と表示されるときは、〈登録して再起動〉をクリックすると、画面上で確定された内容が有効になります。

再起動中は、下記の画面を表示します。

本体を再起動しています。
本体の起動を確認後、[Back]をクリックしてください。

※再起動が完了(約1分)するまで、[Back]と表示された文字の上にマウスポインターを移動してクリックしても、設定画面に戻りませんので、しばらくしてから再度クリックしてください。

※表示画面によって、表示されるボタンの種類や位置が異なります。

2.「LAN側IP」画面

■ 本体名称

「ネットワーク設定」ー**「LAN側IP」**

本製品の名称を設定します。

本体名称: …… 「Telnet」で本製品に接続したとき、ここで設定した本体名称を表示します。 （出荷時の設定：AP-80）

※アルファベットではじまる半角英数字（a ～ z 、A ～Z、0～9、－）を、31文字以内で設定します。
なお、それ以外の文字は、登録できない場合があります。

※「－（ハイフン）」を本体名称の先頭、または末尾に使用すると、登録できません。

■ VLAN設定

「ネットワーク設定」ー**「LAN側IP」**

VLAN機能についての設定です。

マネージメントID: …… 本製品に設定された同じID番号を持つネットワーク上の機器からのアクセスだけを許可できます。
（出荷時の設定：0）

設定できる範囲は、「0～4094」です。

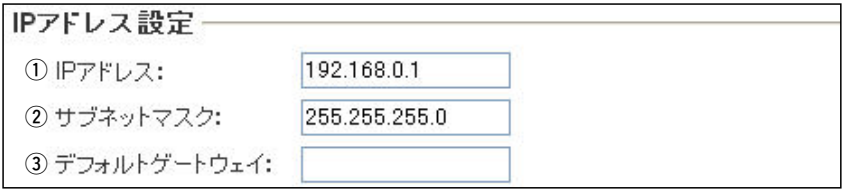
※VLAN IDを使用しないネットワークから本製品にアクセスするときは、「0」を設定します。

※不用意に設定すると、本製品の設定画面にアクセスできなくなりますのでご注意ください。

■ IPアドレス設定

「ネットワーク設定」ー「LAN側IP」

本製品のLAN側IPアドレスを設定します。



①IPアドレス: …… 本製品のIPアドレスを設定します。

（出荷時の設定:192.168.0.1）

本製品を現在稼働中のネットワークに接続するときなど、そのLANに合わせたネットワークアドレスに変更してください。

※本製品のDHCPサーバー機能を使用する場合は、「DHCP」画面にある[DHCPサーバー設定]項目の[割り当て開始IPアドレス]欄(☞P62、P69)についてもネットワーク部を同じ設定にしてください。

②サブネットマスク:

…… 本製品のサブネットマスク(同じネットワークで使用するIPアドレスの範囲)を設定します。

（出荷時の設定:255.255.255.0）

本製品を現在稼働中のネットワークに接続するときなど、そのLANに合わせたサブネットマスクに変更してください。

【例:「255.255.255.248」に設定する場合】

同じネットワークで使用するIPアドレスの範囲は、「192.168.0.0～192.168.0.7」になります。

この場合、端末に割り当てできるIPアドレスの範囲は、「192.168.0.2～192.168.0.6」です。

なお、端末に割り当てできないIPアドレスは次のようになります。

「192.168.0.0」:ネットワークアドレス

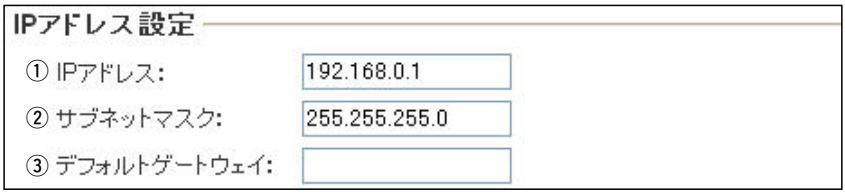
「192.168.0.1」:本製品のLAN側IPアドレス

「192.168.0.7」:ブロードキャストアドレス

2.「LAN側IP」画面

■ IPアドレス設定

「ネットワーク設定」ー**「LAN側IP」**



③デフォルトゲートウェイ:

…… 本製品のIPアドレスとネットワーク部が異なる接続先と通信する場合、パケット転送先機器のIPアドレスを入力します。

※本製品と同じIPアドレスは、登録できません。

3.「DHCPサーバー」画面

■ DHCPサーバー設定

「ネットワーク設定」ー「DHCPサーバー」

DHCPサーバー機能についての設定です。

①DHCPサーバー機能を使用:

…… DHCPサーバー機能の使用を設定します。

(出荷時の設定:しない)

「する」に設定すると、② ～ ⑪の設定が有効になり、本製品に有線および無線で接続している端末がTCP/IP設定を「IPアドレスを自動的に取得する」にしている場合、本製品のDHCPクライアントになります。

②割り当て開始IPアドレス:

…… 本製品に有線および無線で接続する端末へ、IPアドレスを自動で割り当てるときの開始アドレスを設定します。

(出荷時の設定:192.168.0.10)

3.「DHCPサーバー」画面

■ DHCPサーバー設定

「ネットワーク設定」ー**「DHCPサーバー」**

③割り当て個数: …… 本製品が自動割り当てできるIPアドレスの個数を設定します。（出荷時の設定:30）
[割り当て開始IPアドレス]（②）欄に設定されたIPアドレスから連続で自動割り当てできるIPアドレスの最大個数は、0～128（無線LANで接続する端末を含む）までです。
※128個を超える分については設定できませんので、手動でクライアントに割り当ててください。
※「0」を設定したときは、自動割り当てをしません。

④サブネットマスク:
…… [割り当て開始IPアドレス]（②）欄に設定されたIPアドレスに対するサブネットマスクです。
（出荷時の設定:255.255.255.0）

⑤ **リース期間:** …… DHCPサーバーが、ローカルIPアドレスを定期的に自動で端末に割り当てなおす期限を時間で指定します。
（出荷時の設定：72）
設定できる範囲は、「1～9999（時間）」です。

⑥ **ドメイン名:** …… 指定のドメイン名を設定する必要があるときは、DHCPサーバーが有線で接続する端末に通知するネットワークアドレスのドメイン名を127文字（半角英数字）以内で入力します。

⑦ **デフォルトゲートウェイ:**
…… [割り当て開始IPアドレス]（②）欄のIPアドレスとネットワーク部が異なる接続先と通信する場合、パケット転送先機器のIPアドレスを入力します。

⑧ **プライマリーDNSサーバー:**
…… DNSサーバーのアドレスが2つある場合は、優先したい方のアドレスを入力します。
入力すると、設定したDNSサーバーアドレスをDHCPクライアントに通知します。

⑨ **セカンダリーDNSサーバー:**
…… [プライマリーDNSサーバー]（⑧）欄と同様に、DNSサーバーのアドレスが2つある場合は、DNSサーバーアドレスのもう一方を入力します。

⑩ **プライマリーWINSサーバー:**
…… Microsoftネットワークを使ってWINSサーバーを利用する場合は、WINSサーバーアドレスを入力します。
WINSサーバーのアドレスが2つある場合は、優先したい方のアドレスを入力します。

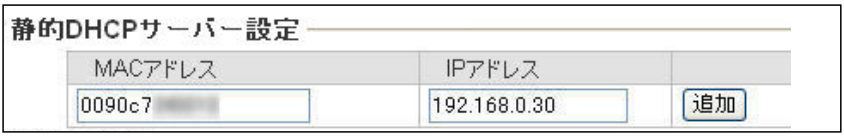
⑪ **セカンダリーWINSサーバー:**
…… 「プライマリーWINSサーバー」と同様、WINSサーバーのアドレスが2つある場合は、残りの一方を入力します。

3.「DHCPサーバー」画面

■ 静的DHCPサーバー設定

「ネットワーク設定」−「DHCPサーバー」

固定IPアドレスを特定の端末に割り当てる設定です。



※画面の値は、入力例です。

静的DHCPサーバー設定

…… 端末のMACアドレスとIPアドレスの組み合わせを登録します。

※本製品のDHCPサーバー機能(☞P62、P69)を使用する場合に有効です。

※入力後は、〈追加〉をクリックしてください。

※最大32個の組み合わせまで登録できます。
登録する端末のIPアドレスは、DHCPサーバー機能による割り当て範囲および本製品のIPアドレスと重複しないように指定してください。

■ 現在の登録

「ネットワーク設定」−「DHCPサーバー」

[静的DHCPサーバー設定]項目で登録した内容を表示します。

※画面の値は、登録例です。

〈削除〉…… 登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

4.「ルーティング」画面

■ IP経路情報

「ネットワーク設定」ー**「ルーティング」**

本製品を起点とするパケットの送信において、そのパケットをどのルーター、またはどの端末に配送すべきかの情報を表示します。

IP経路情報

①宛先	②サブネットマスク	③ゲートウェイ	④経路	⑤作成
127.0.0.0	255.0.0.0	127.0.0.1	lo0	misc
127.0.0.1	255.255.255.255	127.0.0.1	lo0	host
192.168.0.0	255.255.255.0	192.168.0.1	mirror0	misc

※この項目には、現在有効な経路だけを表示します。

①**宛先** …… ルーティングの対象となるパケットの宛先IPアドレスを表示します。

②**サブネットマスク** …… ルーティングの対象となるパケットの宛先IPアドレスに対するサブネットマスクを表示します。

③**ゲートウェイ** …… ルーティングの対象となるパケットの宛先IPアドレスに対するゲートウェイを表示します。

④**経路** …… ルーティングの対象となるパケットの宛先IPアドレスに対する転送先インターフェースを表示します。
◎lo0　：ループバックアドレスを意味するインターフェース
◎mirror0　：インターフェースが本機自身の場合

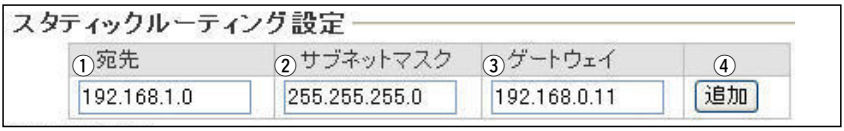
⑤**作成** …… どのように経路情報が作成されたかを表示します。
◎static　：スタティック(定義された)ルートにより作成
◎misc　：ブロードキャストに関係するフレーム処理で作成
◎host　：ホストルートにより作成

4.「ルーティング」画面

■ スタティックルーティング設定

「ネットワーク設定」ー**「ルーティング」**

パケットの中継経路を最大32件まで登録できます。



※画面の値は、入力例です。

①**宛先** …… 対象となる相手先のIPアドレスを入力します。

②**サブネットマスク**…… 対象となる宛先のIPアドレスに対するサブネットマスクを入力します。

③**ゲートウェイ** …… パケット転送先ルーターのIPアドレスを入力します。

④**〈追加〉** …… 入力内容が登録され、[現在の登録]項目に表示します。

■ 現在の登録

「ネットワーク設定」ー**「ルーティング」**

[スタティックルーティング設定]項目で登録した内容を表示します。

※画面の値は、登録例です。

〈削除〉…… 登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

登録したエントリーに該当するパケットを通過させたり、通過を阻止させるフィルターの設定です。

①**番号:** …… フィルターを比較する順位を指定します。
設定できる範囲は、「1～64」です。
本製品が受信、または送信するパケットと[現在の登録]項目に表示されたフィルターと比較します。
※フィルタリングの条件は、1つ以上指定してください。
※番号が指定されていないときは、登録できません。
※IPv6のパケットには対応していません。

【順位と比較について】
フィルターを複数設定しているときは、番号の小さい順番に比較を開始します。
フィルタリングの条件に一致した中から、番号が最小のエントリーで処理をします。
※フィルタリングの条件に一致した時点で、それ以降の識別番号のエントリーは比較しません。

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

②このエントリーを使用:

…… 登録するフィルターの使用について設定します。
（出荷時の設定:しない）
登録だけして使用しないときは、「しない」を選択します。

③ログを表示: …… 「情報表示」メニューの「SYSLOG」画面へのログ表示について設定します。（出荷時の設定:する）

④方法: …… フィルタリングの方法を選択します。
（出荷時の設定:透過）
◎遮断:すべてのフィルタリング条件に一致した場合、そのパケットを破棄します。
◎透過:すべてのフィルタリング条件に一致した場合、そのパケットを通過します。

⑤送信元インターフェース:

…… フィルタリングの対象となる送信元インターフェースを選択します。（出荷時の設定:全て）

◎mirror0　:インターフェースが本機自身の場合
◎ag0　:インターフェースが有線LANの場合
◎ath0～ath3 :インターフェースが本製品の無線LAN（仮想AP）の場合

※「全て」を選択すると、「mirror0」、「ag0」、「ath0～ath3」が送信元インターフェースの対象になります。

⑥宛先インターフェース:

…… フィルタリングの対象となる宛先インターフェースを選択します。（出荷時の設定:全て）

◎mirror0　:インターフェースが本機自身の場合
◎ag0　:インターフェースが有線LANの場合
◎ath0～ath3 :インターフェースが本製品の無線LAN（仮想AP）の場合

※「全て」を選択すると、「mirror0」、「ag0」、「ath0～ath3」が宛先インターフェースの対象になります。

⑦送信元MACアドレス／マスク:

…… フィルタリングの対象となるEthernetヘッダー内において、送信元MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積（AND）が［現在の登録］項目（☞P89）に表示されます。

※登録例については、［宛先MACアドレス／マスク:］（⑧）欄で説明しています。

⑧宛先MACアドレス／マスク:

…… フィルタリングの対象となるEthernetヘッダー内において、宛先MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積（AND）が［現在の登録］項目（☞P89）に表示されます。

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

⑧宛先MACアドレス／マスク:(つづき)

【MACアドレスとマスク値の登録例】

[送信元MACアドレス／マスク:](⑦)欄についても、下記の例を参考にしてください。

例1.) 宛先MACアドレス/マスク

00-90-C7-3C-00-64/(空白)

[現在の登録]項目(☞P89)には、下記の内容で表示します。

00-90-C7-3C-00-64/FF-FF-FF-FF-FF-FF

※マスクを指定しないときは、「FF-FF-FF-FF-FF-FF」として登録されます。

※00-90-C7-3C-00-64に一致するMACアドレスがフィルタリングの対象になります。

⑧宛先MACアドレス／マスク：
…… 【MACアドレスとマスク値の登録例】(つづき)

例2.) 宛先MACアドレス/マスク
00-90-C7-3C-00-64/FF-FF-FF-00-00-00
[現在の登録]項目(☞P89)には、下記の内容で表示します。
00-90-C7-00-00-00/FF-FF-FF-00-00-00
※マスク値「0」との論理積は、「0」になるため、「00-90-C7」部分が一致するMACアドレスがフィルタリング対象になります。

例3.) 宛先MACアドレス/マスク
00-90-C7-3C-00-64/FF-FF-FF-00-00-FF
[現在の登録]項目(☞P89)には、下記の内容で表示します。
00-90-C7-00-00-64/FF-FF-FF-00-00-FF
※00-90-C7-00-00-64～00-90-C7-FF-FF-64までが有効範囲になります。
例2.と同様、マスク「00」の部分は、どんな値のMACアドレスでもフィルタリングの条件に一致する対象となります。

⑨**VLAN ID：** …… フィルタリングの対象となる[VLAN ID]を指定(開始値～終端値)します。
入力できる範囲は、「0～4094」です。
「0」を開始値に指定したときは、範囲指定できません。
※開始値だけを設定したときは、一致するパケットが対象です。
※「0」は、VLANタグのないパケット、およびVLAN IDが「0」のパケットが対象です。
「0」以外は、指定のVLANタグ付きパケットが対象です。

⑩**Ethernetタイプ：** ……フィルタリングの対象となるEthernetタイプ名称(ARP/IP)、または16進数(0000～ffff〈4桁〉)で指定します。 (出荷時の設定:全て)

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で、「ARP」を選択したときは、下記の画面になります。

⑪ARPタイプ: …… フィルタリングの対象となるARPタイプを選択します。
(出荷時の設定:全て)
「全て」、「request」、「reply」、「rrequest」、「rreply」のから選択できます。
※「全て」を選択すると、すべてのARPタイプに該当します。

⑫送信元MACアドレス／マスク:
…… フィルターの対象となるARPヘッダー内において、送信元MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[現在の登録]項目(☞P89)に表示されます。
※登録例については、[宛先MACアドレス／マスク:](⑧)欄で説明しています。

⑬送信元IPアドレス：

…… フィルターの対象となるARPヘッダー内において、送信元IPアドレスの有効範囲(開始値～終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

⑭ターゲットMACアドレス／マスク：

…… フィルターの対象となるARPヘッダー内において、ターゲットMACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[現在の登録]項目(☞P89)に表示されます。
※登録例については、[宛先MACアドレス／マスク:](⑧)欄で説明しています。

⑮ターゲットIPアドレス：

…… フィルターの対象となるARPヘッダー内において、ターゲットIPアドレスの有効範囲(開始値～終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「全て」/「指定」を選択したときは、下記の画面になります。

⑪送信元IPアドレス:

…… フィルターの対象となるIPヘッダー内において、送信元IPアドレスの有効範囲(開始値～終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。
※IPv6には対応していません。

⑫宛先IPアドレス: …… フィルターの対象となるIPヘッダー内において、宛先IPアドレスの有効範囲(開始値～終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。
※IPv6には対応していません。

⑬**IPプロトコル:** …… フィルターの対象となるIPヘッダー内において、パケットのトランスポート層プロトコルを選択します。

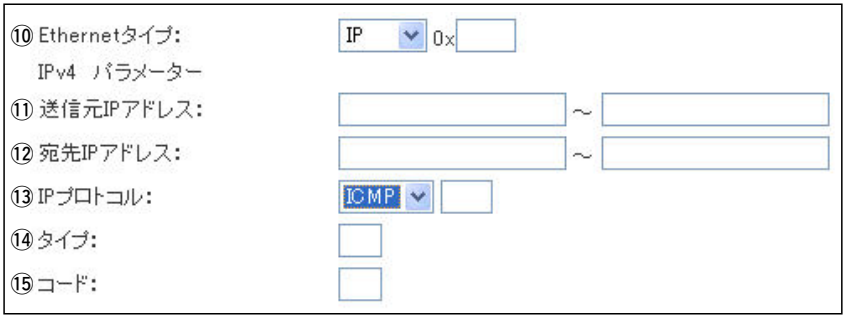
◎全て　:すべてのプロトコルに一致します。
◎ICMP　:ICMPだけに一致します。
◎IGMP　:IGMPだけに一致します。
◎TCP　:TCPだけに一致します。
◎UDP　:UDPだけに一致します。
◎指定　:右のテキストボックスに、IPヘッダーに含まれるパケットのトランスポート層プロトコル番号を入力します。
プロトコル番号は、10進数で0～255までの半角数字を入力します。

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「ICMP」を選択したときは、下記の画面になります。



⑭タイプ: …… フィルタリングの対象となるICMPヘッダー内のタイプを番号(0~255)で指定します。
下記は、代表的なタイプです。

[0] echorep	[9] routerad	[14] timestrep
[3] unreach	[10] routersel	[15] inforeq
[4] squench	[11] timex	[16] inforep
[5] redir	[12] paramprob	[17] maskreq
[8] echo	[13] timest	[18] maskrep

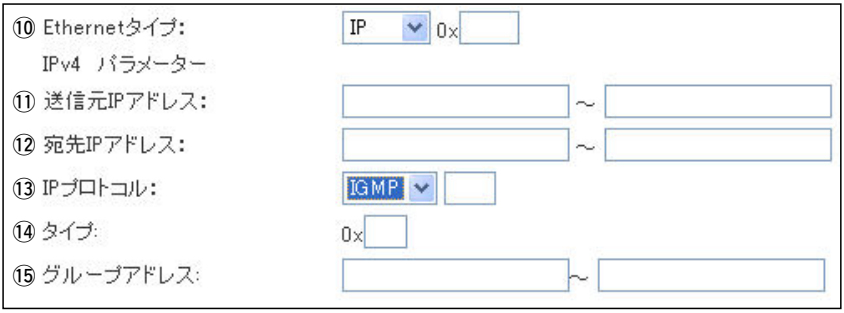
※選択したタイプは、[現在の登録]項目の該当する欄に上記の数字で表示します。
※指定しないときは、すべてがフィルタリングの対象になります。

⑮コード: …… フィルタリングの対象となるICMPヘッダー内のコードを番号(0~255)で指定します。
※割り当てのない番号を指定、または番号を指定しないときは、すべてがフィルタリングの対象になります。

■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「IGMP」を選択したときは、下記の画面になります。



⑭タイプ: …… フィルタリングの対象となるIGMPヘッダー内のタイプを16進数(00~ff〈2桁〉)で指定します。
※指定しないときは、すべてがフィルタリングの対象になります。

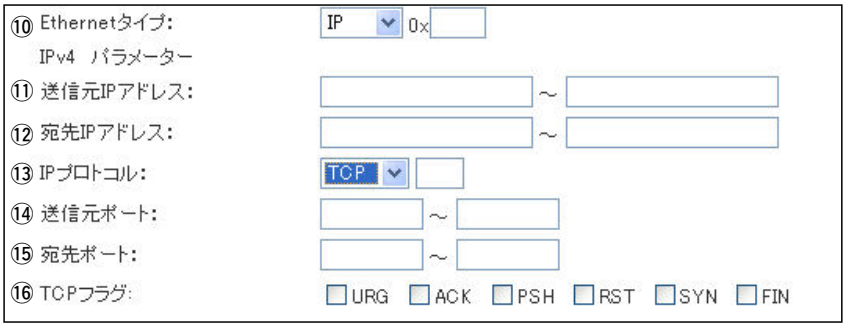
⑮グループアドレス:
…… フィルタリングの対象となるIGMPヘッダー内のマルチキャストグループアドレスの有効範囲(開始値~終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。
※IPv6には対応していません。

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「TCP」を選択したときは、下記の画面になります。



⑭送信元ポート: …… フィルタリングの対象となる送信元TCPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎送信元ポートを指定しないときは、すべてのTCPポート番号がフィルタリングの対象になります。
※TCPヘッダー内のSource Portと比較します。

⑮宛先ポート: …… フィルタリングの対象となる宛先TCPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎宛先ポートを指定しないときは、すべてのTCPポート番号がフィルタリングの対象になります。
※TCPヘッダー内の、Destination Portと比較します。

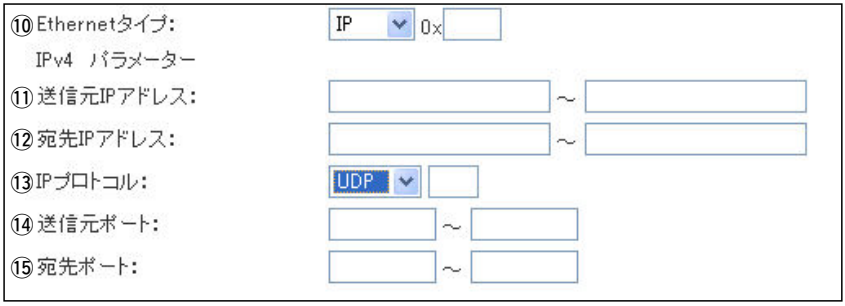
⑯TCPフラグ: …… フィルタリングの対象となるTCPフラグを指定します。
※本製品で指定できるフラグは、URG、ACK、PSH、RST、SYN、FINです。
※TCPヘッダー内のTCPフラグと比較します。
※選択したフラグは、[現在の登録]項目に表示されます。
※何も指定しない場合は、TCPフラグの状態に関係なくフィルタリングの対象になります。
※複数のフラグを選択した場合は、複数のフラグが同時に立っているパケットをフィルタリング対象とします。

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「UDP」を選択したときは、下記の画面になります。



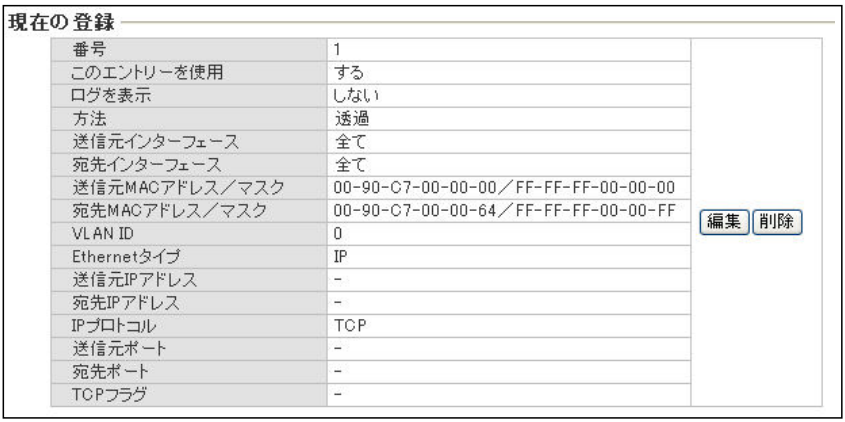
⑭送信元ポート: …… フィルタリングの対象となる送信元UDPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎送信元ポートを指定しないときは、すべてのUDPポート番号がフィルタリングの対象になります。
※UDPヘッダー内のSource Portと比較します。

⑮宛先ポート: …… フィルタリングの対象となる宛先UDPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎宛先ポートを指定しないときは、すべてのUDPポート番号がフィルタリングの対象になります。
※UDPヘッダー内の、Destination Portと比較します。

■ 現在の登録

「ネットワーク設定」ー**「パケットフィルター」**

[パケットフィルター]項目から登録した現在の各エントリーの内容を表示します。



※上記画面の内容は、登録例です。
※未設定の項目には、「-」が表示されます。

〈編集〉…… 左の欄に表示されたエントリーを編集するボタンです。〈編集〉をクリックすると、その左の欄に表示された内容を[パケットフィルター]項目(☞P75)の各欄に表示します。

〈削除〉…… 左の欄に表示されたエントリーを削除するボタンです。〈削除〉をクリックすると、削除されます。

5.「パケットフィルター」画面

■ パケットフィルター使用例

「ネットワーク設定」ー**「パケットフィルター」**

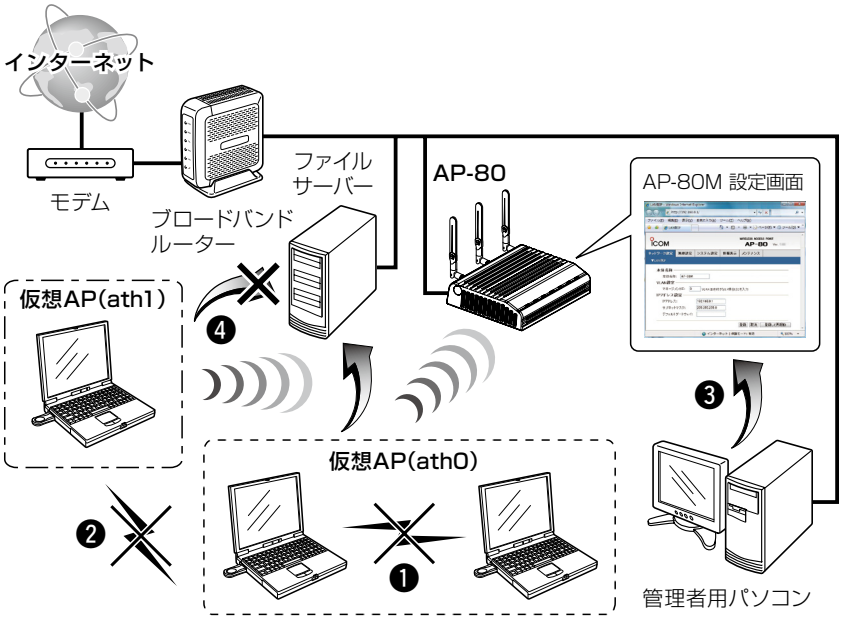
下図とその説明(❶～❹)に示すのような使用例について、パケットフィルターの設定方法を説明します。

❶仮想AP(ath0:VLAN IDなし)内の無線LAN端末同士の通信を禁止するには (☞P91)

❷仮想AP(ath0:VLAN IDなしとath1:VLAN IDなし)間の無線LAN端末同士の通信を禁止するには (☞P92)

❸AP-80の設定画面へのアクセスを管理者用端末に制限するには (☞P93～P94)

❹仮想AP(ath1:VLAN IDなし)からインターネットへの接続を許可し、有線LAN(ファイルサーバーなど)への接続を禁止するには (☞P95)



次ページにつづく➔

■ パケットフィルター使用例

「ネットワーク設定」ー**「パケットフィルター」**

前ページに示す(❶～❹)について、設定例を説明します。

❶仮想AP(ath0:VLAN IDなし)内の無線LAN端末同士の通信を禁止するには
送信元インターフェース、宛先インターフェースともにath0を設定することによりath0に接続した無線端末間通信禁止ができます。
また、MACアドレスを指定しない場合、ath0に接続するすべての無線端末が遮断条件に該当します。

次ページにつづく➔

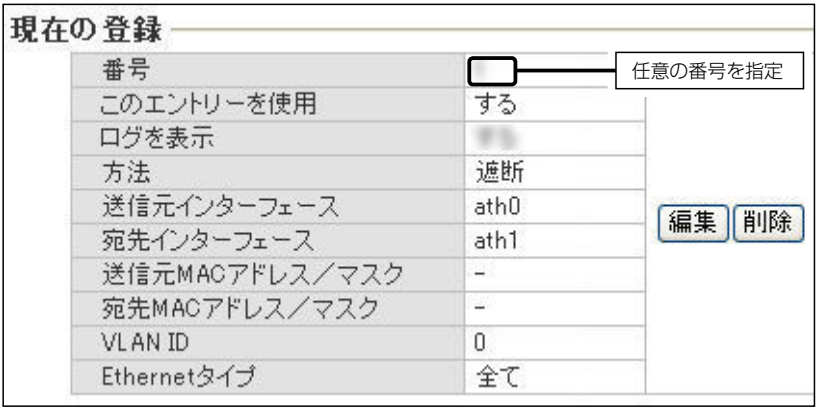
5.「パケットフィルター」画面

■ パケットフィルター使用例

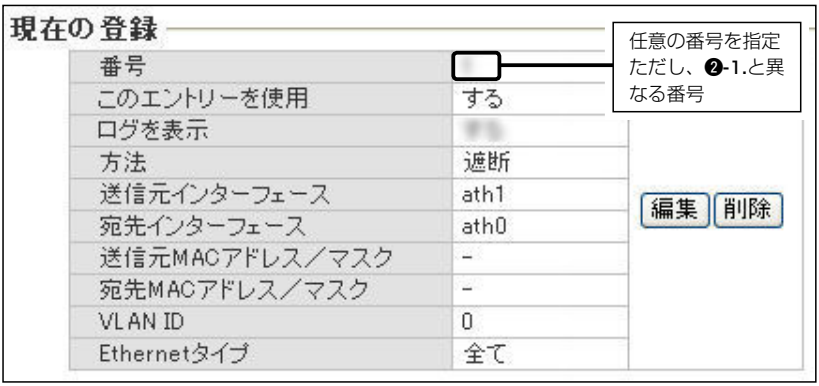
「ネットワーク設定」ー**「パケットフィルター」**

❷仮想AP(ath0:VLAN IDなしとath1:VLAN IDなし)間の無線LAN端末同士の通信を禁止するには

1.仮想AP(ath0)→仮想AP(ath1)方向の通信を遮断



2.仮想AP(ath1)→仮想AP(ath0)方向の通信を遮断



次ページにつづく➔

■ パケットフィルター使用例

「ネットワーク設定」ー**「パケットフィルター」**

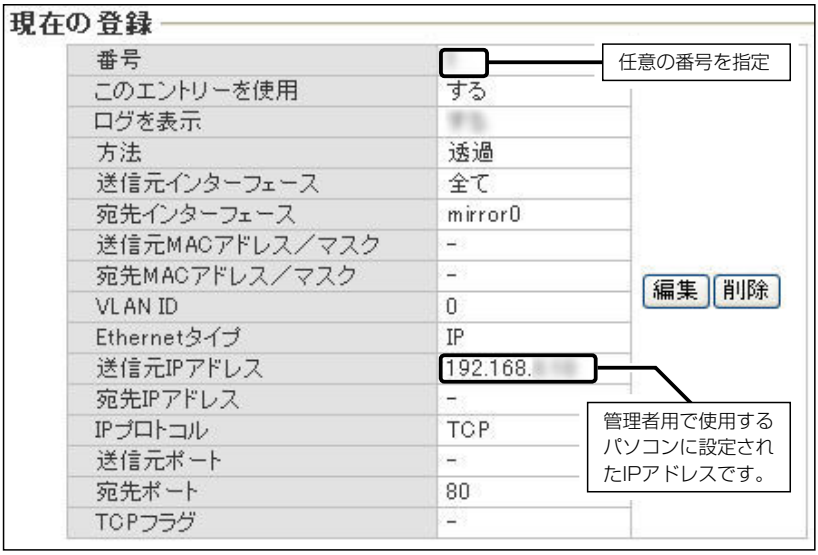
❸AP-80の設定画面へのアクセスを管理者用端末に制限するには

※マネージメントIDが「0」の場合を例に説明しています。

※設定に使用する端末からのWEB画面へのアクセスを妨げないようエントリー追加･削除の順番は、注意してください。

エントリーを追加するときは、透過エントリー→遮断エントリーの順に、エントリーの削除は、遮断エントリー→透過エントリーの順に操作してください。

1.管理用端末からのWEBアクセスを透過



次ページにつづく➔

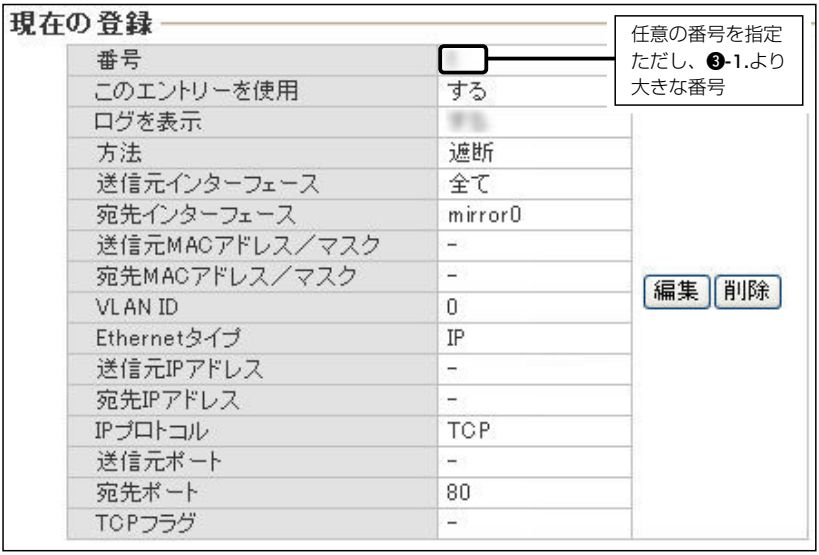
5.「パケットフィルター」画面

■ パケットフィルター使用例

「ネットワーク設定」ー**「パケットフィルター」**

❸AP-80の設定画面へのアクセスを管理者用端末に制限するには（つづき）

2.管理用端末以外からのWEBアクセスを遮断



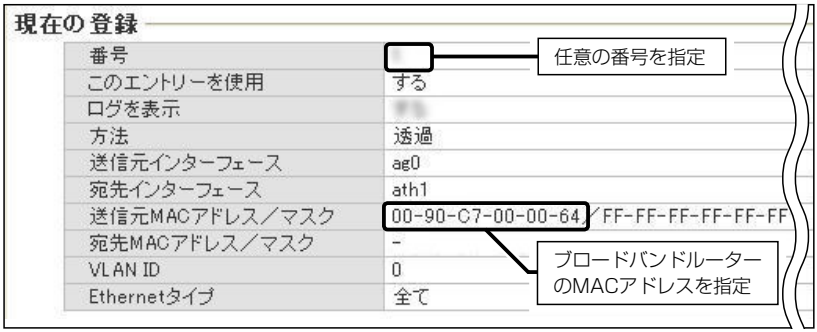
■ パケットフィルター使用例

「ネットワーク設定」ー**「パケットフィルター」**

❹仮想AP(ath1:VLAN IDなし)からインターネットへの接続を許可し、有線LAN(ファイルサーバーなど)への接続を禁止するには

※ブロードバンドルーター以外のDHCPサーバーを使用する場合は、対応する透過エントリーを追加してください。

1.ブロードバンドルーターから仮想AP(ath1)への通信を透過



2.ブロードバンドルーター以外から仮想AP(ath1)への通信を遮断

6.「無線LAN」画面

■ 無線LAN設定

「無線設定」ー**「無線LAN」**

本製品に内蔵された無線LANカードに対する設定です。

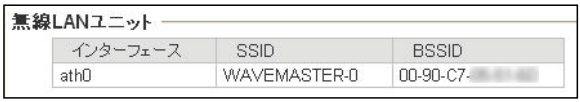
①無線UNITを使用:

…… 無線通信機能の使用を設定します。

(出荷時の設定:する)

「しない」に設定すると、本製品の無線通信機能を停止します。

また、「する」に設定されているときだけ、下記の内容を「情報表示」メニューにある「ネットワーク情報」画面の[無線LANユニット]項目(☞P149)に表示します。



②**チャンネル：** …… 本製品の無線通信に使用するチャンネルを設定します。
（出荷時の設定：001CH（2412MHz）、
□ 40MHz帯域幅モード）

無線LAN端末は、本製品のチャンネルを自動的に検知して通信します。

☑ **40MHz帯域幅モード：**
チェックボックスにチェックマークを入れると、通常（20MHz）の２倍の周波数帯域幅を使用して、最大300Mbps（理論値）の速度で通信します。

□ **40MHz帯域幅モード：**（20MHz帯域幅モード）
チェックボックスのチェックマークをはずしたときは、従来と同じ周波数帯域幅（20MHz）を使用して、最大130Mbps（理論値）の速度で通信します。

下記のように、選択するチャンネルによって、使用できる無線LAN規格が異なります。

「001CH」～「013CH」を選択すると、
[IEEE802.11ｎ/b/g]規格〈2.4GHz帯〉で通信します。 ⇒本書98ページをご覧ください。

「036CH」～「048CH」を選択すると、
[IEEE802.11n/a（W52）]規格〈5.2GHz帯〉で通信します。 ⇒本書100ページをご覧ください。

「052CH」～「064CH」を選択すると、
[IEEE802.11n/a（W53）]規格〈5.3GHz帯〉で通信します。 ⇒本書101ページをご覧ください。

「100CH」～「140CH」を選択すると、
[IEEE802.11n/a（W56）]規格〈5.6GHz帯〉で通信します。⇒本書102ページをご覧ください。

次ページにつづく➔

6.「無線LAN」画面

■ 無線LAN設定

「無線設定」ー**「無線LAN」**

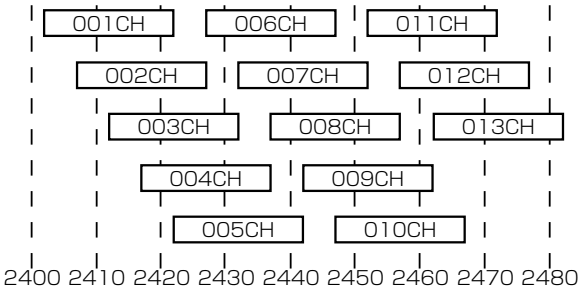
②チャンネル:(つづき)

◎**[IEEE802.11n/b/g]規格について**

「20MHz帯域幅モード」(☞P97)で使用する場合、下図に示すように、帯域の1部が重複するため、近くに[IEEE802.11n/b/g]規格の無線アクセスポイントやビル間通信機器が存在するときは、電波干渉することがあります。

電波干渉を防止するため、本製品の「チャンネル」は、別の無線ネットワークグループと4チャンネル以上空けて設定してください。

たとえば、お互いの設定を、「001CH(2412MHz)」-「006CH(2437MHz)」-「011CH(2462MHz)」にすると電波干渉しません。

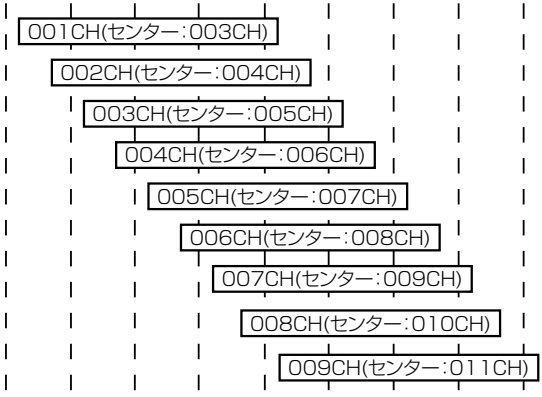


②チャンネル：…… ◎[IEEE802.11n/b/g]規格について （つづき）

「40MHz帯域幅モード」で（☞P97）使用する場合、下図に示すように、2倍の周波数帯域幅（40MHz）の電波を使用するため、「010CH（2457MHz）～013CH（2472MHz）」は設定できません。

さらに、帯域の1部がすべてのチャンネルで重複するため、近くに[IEEE802.11n/b/g]規格で異なるチャンネルの無線アクセスポイントやビル間通信機器が存在するときは、電波干渉することがあります。

電波干渉を防止するときは、「20MHz帯域幅モード」（☞P97）に変更するか、[パワーレベル]（☞P103）、または機器の設置場所を変更してください。



次ページにつづく➔

6.「無線LAN」画面

■ 無線LAN設定

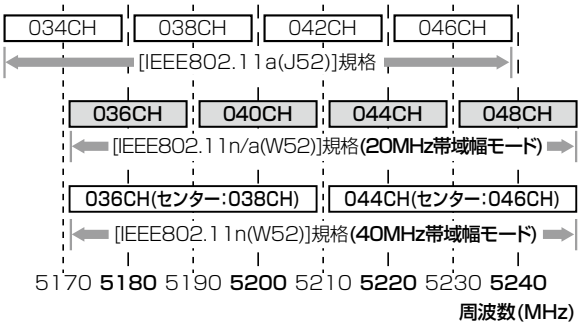
「無線設定」ー**「無線LAN」**

②チャンネル:(つづき)

◎**[IEEE802.11n/a(W52)]規格について**

近くに[IEEE802.11a(J52)]規格で無線LAN端末が稼働しているとき、本製品の[IEEE802.11n/a(W52)]規格の「036CH(5180MHz)～048CH(5240MHz)」をご使用になると、下図に示すように電波干渉の原因になることがありますのでご注意ください。

※「40MHz帯域幅モード」で(☞P97)使用する場合、下図に示すように、2倍の周波数帯域幅(40MHz)の電波を使用するため、「040CH(5200MHz)」と「048CH(5240MHz)」は設定できません。



②チャンネル：…… ◎[IEEE802.11n/a(W52)]規格について(つづき)

※[IEEE802.11a(J52)]規格は、電波法改正(2005年5月)以前の規格のため、本製品では使用できません。

※[IEEE802.11n/a(W52/W53/W56)]規格で通信する場合、お互いを異なるチャンネルに設定すれば、チャンネル間の電波干渉に配慮する必要はありません。

◎**[IEEE802.11n/a(W53)]規格について**

「20MHz帯域幅モード」(☞P97)で使用する場合、「052CH(5260MHz DFS)～064CH(5320MHz DFS)」を選択すると、DFS(Dynamic Frequency Selection)機能が有効になります。

本製品の再起動後や電源投入直後の約1分間は、本製品へのアクセスを停止します。

気象レーダーなど干渉する電波を検出すると、自動的に電波干渉しない「036CH(5180MHz)～048CH(5240MHz)」/「052CH(5260MHz DFS)～064CH(5320MHz DFS)」に変更されます。

なお、変更されたチャンネルが「036CH(5180MHz)～048CH(5240MHz)」の場合は、DFS機能を停止します。

使用しているチャンネルを下図のように表示します。

(DFS機能によりチャンネルが変更されたときの表示例)

※干渉する電波を検出したチャンネルは、約30分間使用できません。

※**「40MHz帯域幅モード」**(☞P97)は、この規格(W53)で使用できません。

次ページにつづく➔

6.「無線LAN」画面

■ 無線LAN設定

「無線設定」ー**「無線LAN」**

②チャンネル:(つづき)

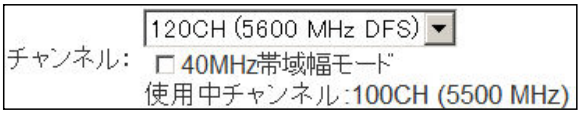
◎**[IEEE802.11n/a(W56)]規格について**

「20MHz帯域幅モード」(☞P97)で使用する場合、「100CH(5500MHz DFS)～140CH(5700MHz DFS)」を選択すると、DFS(Dynamic Frequency Selection)機能が有効になります。

本製品の再起動後や電源投入直後の約1分間は、本製品へのアクセスを停止します。

気象レーダーなど干渉する電波を検出すると、自動的に電波干渉しない「100CH(5500MHz DFS)～140CH(5700MHz DFS)」に変更されます。

使用しているチャンネルを下図のように表示します。



(DFS機能によりチャンネルが変更されたときの表示例)

※干渉する電波を検出したチャンネルは、約30分間使用できません。

また、「100CH(5500MHz DFS)～140CH(5700MHz DFS)」の全チャンネルでレーダーを検出した場合、本製品の無線通信を約30分間停止します。

※**「40MHz帯域幅モード」**(☞P97)は、この規格(W56)で使用できません。

③**パワーレベル：** …… 本製品に内蔵する無線LANカードの送信出力を、高/中/低(3段階)の中から選択します。　(出荷時の設定:高)
本製品の最大伝送距離は、パワーレベルが「高」の場合です。
パワーレベルを低くすると、それに比例して伝送距離も短くなります。

【パワーレベルを低くする目的について】

◎本製品から送信される電波が広範囲に届くのを軽減したいとき
◎通信エリアを制限してセキュリティーを高めたいとき
◎比較的狭いエリアに複数台の無線アクセスポイントが設置された環境で、近くの無線LAN機器との電波干渉をなくして、通信速度の低下などを軽減したいとき

④**DTIM間隔：** …… DTIM(Delivery Traffic Indication Message)をビーコンに挿入する間隔を設定します。　(出荷時の設定:1)
設定できる範囲は、「1～50」です。
DTIMとは、パワーセーブしている端末に対して、ブロードキャスト･マルチキャストパケット配送を伝えるメッセージのことです。
※設定を変更すると、正常に通信できないことがありますので、特に必要がない場合は、工場出荷時の状態でご使用ください。

⑤**プロテクション機能：**
…… 異なる無線LAN規格の混在による電波干渉をなくして、無線LANの通信速度低下を軽減したいとき有効な設定です。　(出荷時の設定:有効)
※「有効」に設定すると、[IEEE802.11n/a(W52/W53/W56)/b/g]規格の通信速度低下を防止でき、極端に通信速度が遅い場合に効果があります。
※接続する無線LAN端末が少ない場合、または周囲にほかの無線LAN機器が存在しない場合には、「無効」に設定してください。

7.「仮想AP」画面

■ 仮想AP設定

「無線設定」ー**「仮想AP」**

本製品1台で複数の仮想無線アクセスポイントとして使用するための設定です。

①インターフェース:

設定する仮想AP(アクセスポイント)の名称(ath0～ath3)を選択します。 (出荷時の設定:ath0)
選択するインターフェースごとに、[仮想AP設定]項目(②～⑦)と[暗号化設定]項目(☞P108)の設定内容を変更できます。

※仮想APの名称(ath0～ath3)は、変更できません。

※「ath1～ath3」を使用するときは、[仮想APを使用](②)欄(☞P105)の設定を「する」に変更してください。

※「MACアドレスフィルタリング」画面(☞P58、P120)についても、仮想APごとに設定できます。

※ご使用のWWWブラウザーでJavaScript®が「無効」に設定されていると、仮想APの名称を選択したとき、[仮想AP設定]項目(②～⑦)と[暗号化設定]項目(☞P108)の設定内容が更新されません。
更新されないときは、ご使用のWWWブラウザーでJavaScript®の設定が「有効」に設定されていることを確認してください。

②仮想APを使用： …… [インターフェース]（①）欄で選択した仮想AP（ath0～ath3）の使用について設定します。

（出荷時の設定：ath0選択時→する
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない）

※「ath0」は、設定を「しない」に変更できません。
※通信速度低下を防止するため、使用する無線インターフェースだけを「する」に設定してください。

③SSID： …… [インターフェース]（①）欄で選択した仮想AP（ath0～ath3）の[SSID]を設定します。
大文字/小文字の区別に注意して、任意の半角英数字32文字以内で入力します。

（出荷時の設定：ath0選択時→WAVEMASTER-0
ath1選択時→WAVEMASTER-1
ath2選択時→WAVEMASTER-2
ath3選択時→WAVEMASTER-3）

※[SSID]は、無線ネットワークのグループ分けをするために使用します。
[SSID]の異なる無線LAN端末とは接続できません。
※無線アクセスポイントが無線伝送エリア内に複数存在しているような場合、個々の無線ネットワークグループを[SSID（無線ネットワーク名）]で識別できます。
※「ath0」～「ath3」の仮想APで[SSID]が重複している場合は、その仮想APを使用できません。
※[SSID]と[ESSID]は、同じ意味で使用しています。
本製品以外の無線LAN機器では、[ESSID]と表記されている場合があります。

「仮想AP」画面で設定を変更するときのご注意

別の仮想APと併せて設定するときは、〈登録〉、または〈登録して再起動〉を操作してから、別の仮想APを選択してください。
〈登録〉または、〈登録して再起動〉の操作をしないで別の仮想APを選択したときは、変更する前の設定内容に戻ります。

7.「仮想AP」画面

■ 仮想AP設定

「無線設定」ー**「仮想AP」**

④VLAN ID: …… [インターフェース](①)欄で選択した仮想AP(ath0～ath3)が所属する無線グループのID番号を設定します。
(出荷時の設定:0)
設定できる範囲は、「0～4094」です。
※[VLAN ID]を付けないときは、「0」を設定します。
※異なるID番号のネットワークとは通信できません。

⑤ANY接続拒否: …… [インターフェース](①)欄で選択した仮想AP(ath0～ath3)と「ANY」モード(アクセスポイント自動検索接続機能)で通信する無線LAN端末(弊社製無線LANカード:SL-11やSL-110を除く)からの検索や接続の拒否についての設定です。 (出荷時の設定:しない)
出荷時の設定では、接続が簡単になるように、無線LAN端末からの検索や接続を許可しています。
この設定を「する」にした場合、「ANY」モードで通信する無線LAN端末が使用する「Windows Vista/Windows XP標準のワイヤレスネットワーク接続」や「弊社製無線LANカードに付属の設定ユーティリティー」から検索されません。
※WPS機能(☞P22、P137)との併用は、できません。

⑥接続端末制限：…… [インターフェース]（①）欄で選択した仮想AP（ath0～ath3）に同時接続可能な無線LAN端末の台数を設定します。（出荷時の設定：63）
設定できる範囲は、「1～63」です。
接続制限を設定すると、接続が集中するのを防止（本製品の負荷を分散）できますので、接続集中による通信速度低下を防止できます。

⑦アカウンティングを使用：
…… [インターフェース]（①）欄で選択した仮想AP（ath0～ath3）と通信する無線LAN端末のネットワーク利用状況（接続、切断、MACアドレスなど）を収集してアカウンティングサーバーに送信する機能の使用を設定します。（出荷時の設定：しない）

7.「仮想AP」画面

■ 暗号化設定

「無線設定」ー**「仮想AP」**

各仮想AP(ath0～ath3)の暗号化設定をします。

※選択する設定内容(①、②)に応じて、上記以外の設定(③～⑦)を表示(☞P113～P117)します。

①ネットワーク認証:

…… [暗号化方式](②)欄で選択された暗号化方式を使用する無線LAN端末からのアクセスに対する認証方式を選択します。　(出荷時の設定:オープンシステム・共有キー)

※異なる認証方式の相手とは互換性がありませんので、通信をする相手間で同じ設定にしてください。

※弊社製無線LAN機器によっては、「認証モード」と記載されています。

【認証方式について】

◎オープンシステム・共有キー:

「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、「オープンシステム」と「共有キー」を自動認識しますので、本製品と暗号鍵(キー)が同じであれば通信できます。

◎オープンシステム:

「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、暗号鍵(キー)の認証をしません。

◎共有キー:

「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、本製品と無線LAN端末の暗号鍵(キー)が同じかどうかを認証します。

①ネットワーク認証：(つづき)

……【認証方式について】(つづき)

◎IEEE802.1X：

「WEP RC4」暗号化方式を使用して、RADIUSサーバーによるIEEE802.1X認証するときの設定です。

※「認証サーバー」画面(☞P118)と併せて設定してください。

◎WPA(Wi-Fi Protected Access)：

「TKIP」/「AES」暗号化方式を使用して、RADIUSサーバーによるIEEE802.1X認証をするときの設定です。

※[IEEE802.1X]認証より強力で、「TKIP」暗号化方式の使用を標準規格とする認証方式です。

※「認証サーバー」画面(☞P118)と併せて設定してください。

◎WPA2：

ネットワーク認証方式にWPA2を使用します。

※[WPA]認証より強力な「AES」暗号化方式の使用を標準規格とする認証方式で、「PMKIDキャッシュ」により、再接続による認証が不要です。

※「WPA2」認証に対応したクライアントが必要です。

※「認証サーバー」画面(☞P118)と併せて設定してください。

◎WPA・WPA2：

「WPA」認証と「WPA2」認証を自動認識します。

◎WPA-PSK(Pre-Shared Key)：

共有鍵(キー)で認証します。

RADIUSサーバーを利用しない簡易的な「TKIP」/「AES」暗号化の認証方式で、本製品と無線LAN端末の共有鍵(キー)が同じかどうかを認証します。

◎WPA2-PSK：

ネットワーク認証方式にWPA2-PSKを使用します。

※「WPA2-PSK」認証に対応した無線LAN端末が必要です。

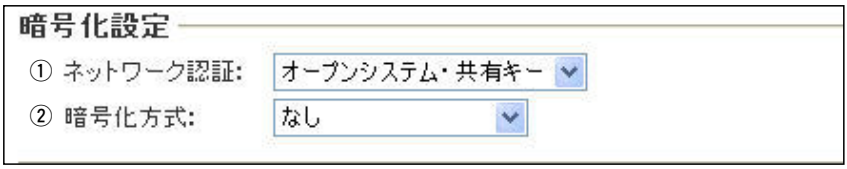
◎WPA-PSK・WPA2-PSK：

「WPA-PSK」認証と「WPA2-PSK」認証を自動認識します。

7.「仮想AP」画面

■ 暗号化設定

「無線設定」ー**「仮想AP」**



※選択する設定内容(①、②)に応じて、上記以外の設定(③～⑦)を表示(☞P113～P117)します。

②暗号化方式: …… 無線伝送データを暗号化する方式を選択します。
(出荷時の設定:なし)

対応する暗号化方式は、「WEP RC4」、「TKIP」、「AES」です。

異なる暗号化方式の相手とは互換性がありませんので、暗号化方式は、通信をする相手間で同じ設定にしてください。

※「WEP RC4 152(128)]方式での接続は、弊社製無線LANカードに付属の設定ユーティリティーをご使用いただくか、弊社製WIRELESS LAN UNIT(SU-80、SE-80、SE-80Mなど)をご用意ください。

【暗号化方式について】

◎なし:

データを暗号化しないで通信します。

※[ネットワーク認証](①)欄で、「オープンシステム・共有キー」、または「オープンシステム」を選択したとき使用できます。

※[IEEE802.11n/a/b/g]規格に準拠します。

※暗号化を設定されることをおすすめします。

【ネットワーク認証と暗号化方式の対応について】

	オープンシステム	共有キー	オープンシステム 共有キー	WPA WPA2	WPA-PSK WPA2-PSK	IEEE802.1X
なし	○	×	○	×	×	×
WEP RC4	○	○	○	×	×	○
TKIP	×	×	×	○	○	×
AES	×	×	×	○	○	×

②暗号化方式：…… 【暗号化方式について】(つづき)

◎WEP RC4：

無線通信で一般によく使用されるセキュリティーです。

※暗号鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

※[ネットワーク認証](①)欄で、「オープンシステム・共有キー」、または「オープンシステム」、「共有キー」、「IEEE802.1X」を選択したとき使用できます。

※「WEP RC4 152(128)」方式は、Windows Vista/Windows XP標準のワイヤレスネットワーク接続を使用して本製品に接続できません。

※[IEEE802.11a/b/g]規格に準拠します。

◎TKIP(Temporal Key Integrity Protocol)：

暗号鍵(キー)を一定時間間隔で自動更新しますので、「WEP RC4」より強力です。

Windows XP(修正プログラムをService Pack1に適用)、またはWindows XP(Service Pack2以降)、Windows Vistaの端末で使用できます。

※[ネットワーク認証](①)欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

※[IEEE802.11a/b/g]規格に準拠します。

※無線LAN端末としてご使用いただける「TKIP」対応の弊社製品については、「暗号化対応表」(☞P178)をご覧ください。

7.「仮想AP」画面

■ 暗号化設定

「無線設定」ー**「仮想AP」**

※選択する設定内容(①、②)に応じて、上記以外の設定(③～⑦)を表示(☞P113～P117)します。

②暗号化方式:…… 【暗号化方式について】(つづき)

◎AES(Advanced Encryption Standard):

暗号化の強化、および暗号鍵(キー)を一定時間間隔で自動更新しますので、「TKIP」より強力な暗号化方式です。

※[ネットワーク認証](①)欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

※[IEEE802.11n/a/b/g]規格に準拠します。

※無線LAN端末としてご使用いただける「AES」対応の弊社製品については、「暗号化対応表」(☞P178)をご覧ください。

◎TKIP・AES:

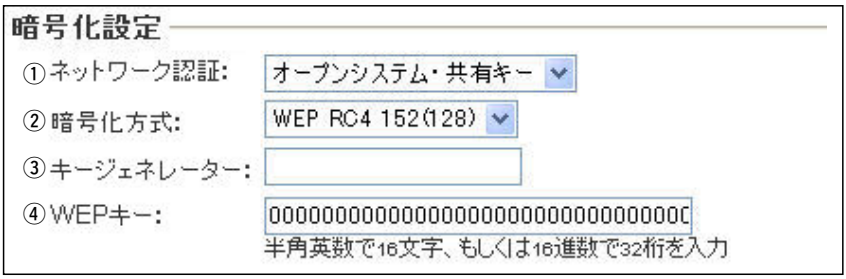
無線LAN端末からのアクセスに対して、「TKIP」と「AES」を自動認識します。

※[ネットワーク認証](①)欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

※「AES」が認識されたときだけ、[IEEE802.11n]規格で通信できます。

■ 暗号化設定

「無線設定」ー**「仮想AP」**



※選択する設定内容(①、②)に応じて、上記以外の設定(⑤～⑦)を表示(☞P116～P117)します。

③キージェネレーター:

…… 暗号化、および復号に使用する16進数の暗号鍵(キー)を[WEPキー:]欄(④)に生成するための文字列を入力します。　(出荷時の設定:空白〈何も設定されていません。〉)

次の順番に操作すると、設定できます。

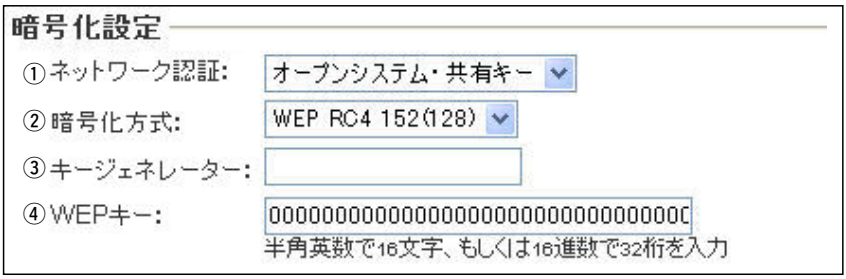
1. [ネットワーク認証](①)欄で、「オープンシステム・共有キー」、または「オープンシステム」、「共有キー」を選択します。
2. [暗号化方式](②)欄で、「WEP RC4 64(40)」、「WEP RC4 128(104)」、「WEP RC4 152(128)」を選択します。
   - ●[キージェネレーター:]欄と[WEPキー:](④)欄を表示します。
3. 大文字/小文字の区別に注意して、文字列を[キージェネレーター:]欄に31文字以内(任意の半角英数字/記号)で入力します。
   - ●入力した文字列より生成された16進数の暗号鍵(キー)を[WEPキー](④)欄に表示します。

次ページにつづく➔

7.「仮想AP」画面

■ 暗号化設定

「無線設定」ー**「仮想AP」**



※選択する設定内容(①、②)に応じて、上記以外の設定(⑤～⑦)を表示(☞P116～P117)します。

③キージェネレーター:(つづき)

…… ※[暗号化方式](②)欄(☞P110)で、「WEP RC4」の暗号化方式を選択したとき、設定できます。

※暗号鍵(キー)を直接入力する場合は、キージェネレーターに文字列が残っていると、[WEPキー:]欄(④)に直接入力できませんので、削除してください。

※入力する文字列は、通信する相手(弊社製機器)側のキージェネレーターと同じ文字列を設定してください。
他社製の機器とは互換性がありませんので、ご注意ください。

※キージェネレーターから生成された暗号鍵(キー)が通信相手間で異なる場合、暗号化されたデータを復号できません。

※[WEPキー](④)欄に表示される暗号鍵(キー)の桁数、および文字数は、[暗号化方式](②)欄の設定によって異なります。(☞P47)

④**WEPキー：** …… [キージェネレーター](③)欄を使用しないで、暗号鍵(キー)を直接設定するとき入力します。

※「0～9」および「a ～f(またはA ～F)」の16進数、またはASCII文字で、半角入力してください。

※入力する暗号鍵(キー)の桁数は、[暗号化方式](②)欄を設定したとき表示される桁数(10桁の表示例:0000000000)と同じに設定してください。
ASCII文字で入力する場合は、16進数の半分(例:5文字)で入力してください。

※本製品には、キーインデックスの設定がなく、「1」に相当します。
Windows XP(Service Pack適用済み)やWindows Vista標準のワイヤレスネットワーク接続(ゼロコンフィグレーション)を使用して、「WEP RC4」で暗号化された本製品と通信する場合、無線LAN端末側のキーインデックスを「1」に設定してください。
なお、Windows XPでService Packが適用されていない場合は、「0」に設定してください。

7.「仮想AP」画面

■ 暗号化設定

「無線設定」ー**「仮想AP」**

※選択する設定内容(①、②)に応じて、上記以外の設定(③、④、⑦)を表示します。
(☞P113、P115、P117)

⑤PSK(Pre-Shared Key):

…… 共有鍵(キー)を半角英数字で入力します。
(出荷時の設定:00000000)
※[ネットワーク認証](①)欄で「WPA-PSK」、「WPA2-PSK」、「WPA-PSK·WPA2-PSK」を選択したとき、設定できます。
※同じ暗号化方式を使用する相手と、同じ共有鍵(キー)を設定してください。
※16進数で設定するときは、64桁を入力してください。
※ASCII文字で設定するときは、大文字/小文字の区別に注意して、8~63文字を入力してください。

⑥WPAキー更新間隔:

…… [ネットワーク認証](①)欄で、「WPA」、「WPA2」、「WPA·WPA2」、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK·WPA2-PSK」を選択したとき、暗号鍵(キー)の更新間隔を分で設定します。 (出荷時の設定:120)
設定できる範囲は、「0~1440(分)」です。
※「0」を設定すると、更新しません。

■ 暗号化設定

「無線設定」ー**「仮想AP」**

※選択する設定内容(①、②)に応じて、上記以外の設定(③～⑥)を表示(☞P113～P116)します。

⑦**再認証間隔:** …… [ネットワーク認証](①)欄で、「IEEE802.1X」を選択したとき、RADIUSサーバーに再度認証を要求する間隔を分で設定します。 (出荷時の設定:120)
設定できる範囲は、「0～9999(分)」です。
※「0」を設定したときは、再認証しません。

8.「認証サーバー」画面

■ RADIUS設定

「無線設定」ー**「認証サーバー」**

RADIUSサーバーを使用してWPA認証、またはIEEE802.1X認証するときの設定です。
◎各仮想AP（ath0～ath3）で共通の設定です。
◎EAP-TLSとEAP-TTLS、EAP-PEAPに対応しています。

①プライマリー/セカンダリー:
…… [プライマリー]列に設定したサーバーから応答がない場合、その次にアクセスさせるRADIUSサーバーがあるときは、[セカンダリー]列にそのRADIUSサーバーアドレスを設定します。

②アドレス: …… 対象となるRADIUSサーバーのIPアドレスを入力します。

③ポート: …… 対象となるRADIUSサーバーの認証ポートを設定します。（出荷時の設定：1812）
※設定できる範囲は、「1～65535」です。
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

④シークレット: …… 本製品とRADIUSサーバーの通信に使用するキーを設定します。
RADIUSサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

■ アカウンティング設定

「無線設定」ー**「認証サーバー」**

セッション中に使用されたリソースの量(接続、切断、MACアドレスなど)をアカウンティングサーバーに送信する設定です。
◎各仮想AP(ath0～ath3)で共通の設定です。

①プライマリー/セカンダリー:
…… [プライマリー]列に設定したサーバーから応答がない場合、その次にアクセスさせるアカウンティングサーバーがあるときは、[セカンダリー]列にそのアカウンティングサーバーアドレスを設定します。

②アドレス: …… 対象となるアカウンティングサーバーのIPアドレスを入力します。

③ポート: …… 対象となるアカウンティングサーバーのポートを設定します。 (出荷時の設定:1813)
※設定できる範囲は、「1～65535」です。
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

④シークレット: …… この欄に設定されたキーを使用して、本製品とサーバー間の通信をします。
アカウンティングサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

9.「MACアドレスフィルタリング」画面

■ MACアドレスフィルタリング設定

「無線設定」ー**「MACアドレスフィルタリング」**

各仮想AP(ath0～ath3)に接続できる無線LAN端末を制限する設定です。

①インターフェース:

…… 設定する仮想AP(アクセスポイント)の名称(ath0～ath3)を選択します。　(出荷時の設定:ath0)
選択するインターフェースごとに、[MACアドレスフィルタリング設定]項目(②、③)と[現在の登録]項目(☞P123)に登録された内容を変更できます。
※表示される名称(ath0～ath3)は、変更できません。
※使用するときは、[MACアドレスフィルタリングを使用:](②)欄の設定を「する」に変更してください。
※ご使用のWWWブラウザーでJavaScript®が「無効」に設定されていると、「ath0」～「ath3」を選択したとき、MACアドレスフィルタリング設定]項目(②、③)と[現在の登録]項目に登録された内容が更新されません。
更新されないときは、ご使用のWWWブラウザーでJavaScript®の設定が「有効」に設定されていることを確認してください。

②MACアドレスフィルタリングを使用:

…… [インターフェース:](①)欄で選択した仮想AP(ath0～ath3)について、MACアドレスフィルタリング機能の使用を設定します。 (出荷時の設定:しない)

※「する」に設定すると、[フィルタリングポリシー:](③)欄の設定、および[現在の登録]項目(☞P123)に登録された内容が有効になります。

※選択した仮想APで使用するときは、「仮想AP」画面から該当する仮想APに対する[仮想APを使用:]欄(☞P105)を「する」に設定された仮想APで有効になります。

③フィルタリングポリシー:

…… [現在の登録]項目(☞P123)に登録された無線LAN端末との無線通信を許可する対象とするか拒否する対象とするかを設定します。 (出荷時の設定:許可リスト)

◎「許可リスト」:MACアドレスが登録された無線LAN端末だけが、本製品と無線通信できます。

※通信を拒否する対象は、MACアドレスを登録していないすべての無線LAN端末です。

◎「拒否リスト」:MACアドレスが登録された無線LAN端末だけが、本製品と無線通信できません。

※通信を許可する対象は、MACアドレスを登録していないすべての無線LAN端末です。

9.「MACアドレスフィルタリング」画面

■ 端末MACアドレスリスト

「無線設定」ー**「MACアドレスフィルタリング」**

各仮想AP(ath0～ath3)について、MACアドレスフィルタリング(☞P58、P120)の対象となる無線LAN端末のMACアドレスを登録します。

MACアドレス: …… MACアドレスフィルタリングの対象となる無線LAN端末のMACアドレスを入力します。
入力後は、〈追加〉をクリックすると、[現在の登録]項目(☞P123)に表示します。
※対象となる無線LAN端末のMACアドレスが[現在の登録]項目から登録できないときに使用します。
※最大256台分のMACアドレスを登録できます。
※入力は半角英数字で12桁(16進数)を入力します。
※2つの入力例は、同じMACアドレスになります。
(入力例:00-90-c7-00-00-10、0090c7000010)
※[MACアドレスフィルタリング設定]項目の[インターフェース:]欄(☞P120)で選択した仮想AP(ath0～ath3)について、MACアドレスフィルタリングが有効なとき、[現在の登録]項目に登録された無線LAN端末との通信を[フィルタリングポリシー:]欄(☞P121)の設定にしたがって制御します。

■ 現在の登録

「無線設定」ー「MACアドレスフィルタリング」

各仮想AP(ath0～ath3)について、MACアドレスフィルタリング(☞P58、P120)の対象となる無線LAN端末の登録と通信状態を表示する画面です。

◆[フィルタリングポリシー:]を「許可リスト」で使用した場合

◆[フィルタリングポリシー:]を「拒否リスト」で使用した場合

①**登録済みの端末** …… 登録されている無線LAN端末のMACアドレスを表示します。

②**受信中の端末** …… 本製品の無線伝送領域内で通信している無線LAN端末のMACアドレスを表示します。

③**通信状況** …… 本製品との無線通信状況を表示します。

「通信中」　:本製品と無線通信中のとき、〈通信中〉とボタンで表示します。
※〈通信中〉をクリックすると、無線通信状態を別画面(☞P125)で表示します。

「通信不許可」:本製品により無線通信が拒否されているときの表示です。

「登録済」　:MACアドレスが登録済みで、無線通信をしていないときの表示です。

9.「MACアドレスフィルタリング」画面

■ 現在の登録　「無線設定」―「MACアドレスフィルタリング」

◆[フィルタリングポリシー:]を「許可リスト」で使用した場合

現在の登録

① 登録済みの端末	② 受信中の端末	③ 通信状況	④
	00-90-C7-00-00-10	通信不許可	追加
00-90-C7-00-00-20	00-90-C7-00-00-20	通信中	削除
00-90-C7-00-00-30		登録済	削除

◆[フィルタリングポリシー:]を「拒否リスト」で使用した場合

現在の登録

① 登録済みの端末	② 受信中の端末	③ 通信状況	④
	00-90-C7-00-00-10	通信中	追加
00-90-C7-00-00-20	00-90-C7-00-00-20	通信不許可	削除
00-90-C7-00-00-30		登録済	削除

④**〈追加〉/〈削除〉** …… [現在の登録] 項目に表示されている無線LAN端末のMACアドレスを端末MACアドレスリストに追加、または端末MACアドレスリストから削除するボタンです。

■ 無線通信状態

「無線設定」ー「MACアドレスフィルタリング」

無線LAN端末との通信状況をモニターします。

※[現在の登録]項目(☞P123)に〈通信中〉ボタンが表示されている場合、そのボタンをクリックすると表示します。

①**通信状況**:…… 「未接続」/「通信中」/「認証中」/「認証失敗」など、接続状況を表示します。
※「通信不可」を表示する場合は、お買い上げの販売店、または弊社サポートセンターにお問い合わせください。

②**MACアドレス**:…… 無線LAN端末のMACアドレスを表示します。

③**SSID**:…… 無線LAN端末のSSIDを表示します。

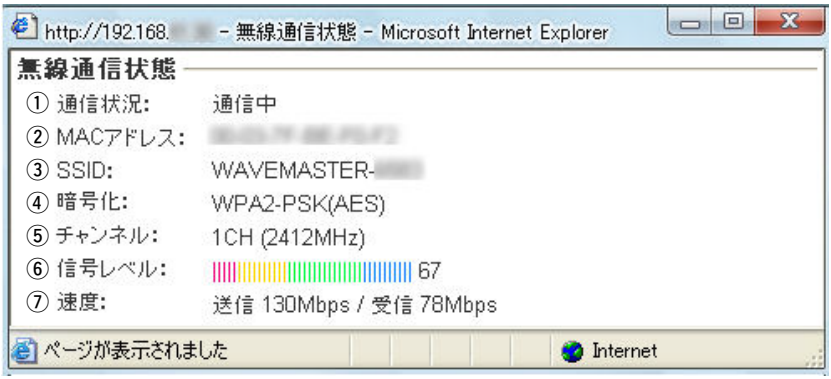
④**暗号化**:…… 無線LAN端末との通信に使用している認証モード・暗号化方式を表示します。

⑤**チャンネル**:…… 無線LAN端末との通信に使用しているチャンネルを表示します。

9.「MACアドレスフィルタリング」画面

■ 無線通信状態

「無線設定」ー**「MACアドレスフィルタリング」**



※[現在の登録]項目(☞P123)に〈通信中〉ボタンが表示されている場合、そのボタンをクリックすると表示します。

⑥**信号レベル**: …… 無線LAN端末から受信した電波信号の強さを、メーターと数値で表示します。
安定した通信の目安は、「緑(15)」以上のレベルです。

表　示	[赤]	[黄]	[緑]	[青]
レベル	0～4	5～14	15～29	30以上

⑦**速度**: …… 本製品の通信速度を理論値(Mbps)で表示します。

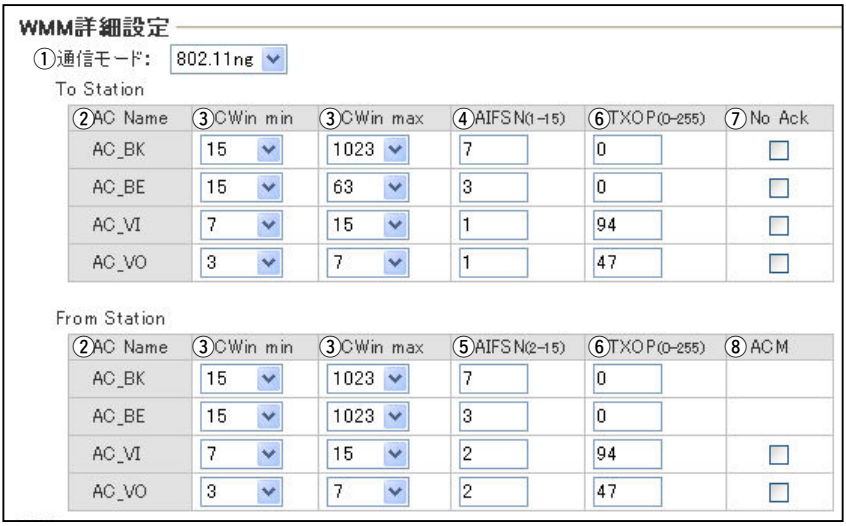
10.「WMM詳細」画面

■ WMM詳細設定

「無線設定」ー**「WMM詳細」**

本製品のWMM機能を使用した無線LAN通信において、[To Station]は、本製品から各無線LAN端末へのデータに対する優先度を設定するEDCA(Enhanced Distributed Channel Access)パラメーターの設定です。

[From Station]は、各無線LAN端末から本製品へのデータに対する優先度を設定するEDCA(Enhanced Distributed Channel Access)パラメーターの設定です。



①通信モード: …… WMM機能の詳細設定(② ～ ⑧)をする無線通信モードを選択します。 (出荷時の設定:802.11ng)

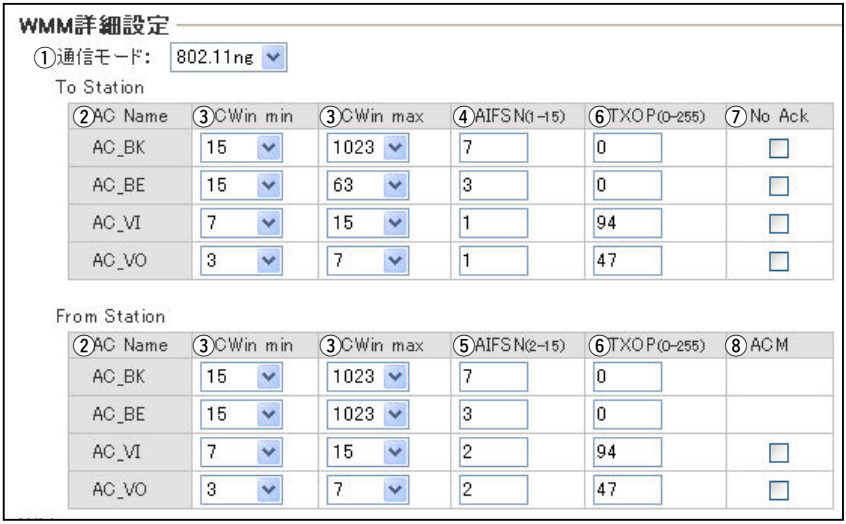
※無線LAN規格(802.11ng/802.11na)ごとに、[To Station]と[From Station]に異なる値を設定できます。

次ページにつづく➔

10.「WMM詳細」画面

■ WMM詳細設定

「無線設定」ー**「WMM詳細」**


WMM詳細設定
①通信モード: 802.11ng
To Station
②AC Name ③CWin min ③CWin max ④AIFSN(1-15) ⑥TXOP(0-255) ⑦No Ack
AC_BK 15 1023 7 0
AC_BE 15 63 3 0
AC_VI 7 15 1 94
AC_VO 3 7 1 47
From Station
②AC Name ③CWin min ③CWin max ⑤AIFSN(2-15) ⑥TXOP(0-255) ⑧ACM
AC_BK 15 1023 7 0
AC_BE 15 1023 3 0
AC_VI 7 15 2 94
AC_VO 3 7 2 47

②**AC Name:** …… WMM(Wi-Fi Multimedia)で規定されるAC(Access Category)の名称で、各アクセスカテゴリー(AC_BK、AC_BE、AC_VI、AC_VO)ごとに、EDCAパラメーター(③～⑥)を設定できます。
EDCAパラメーター(③～⑥)の各値は、Wi-Fiで定められたアクセスカテゴリーの優先順位[AC_BK(低い)、AC_BE(通常)、AC_VI(優先)、AC_VO(最優先)]となるよう設定されています。

〈ご注意〉
EDCAパラメーター(③～⑥)の各値は、一般的な使用で変更する必要はありません。
なお、変更が必要な場合でも、原則としてWi-Fiで定められたアクセスカテゴリーの優先順位を保つように設定してください。
優先順位を変更した場合、ACM(☞P131)などの制御が正しく動作しない場合があります。

③CWin min/CWin max：

…… CWin(Contention Window)の最小値(min)/最大値(max)を設定します。
チャンネルが一定期間未使用になったあとの送信タイミングをContention Windowから乱数で選択することで、[IEEE802.11]規格でのフレーム衝突を回避します。
設定値が小さいほど優先順位が上がり、設定値が大きいほど優先順位が下がります。

（出荷時の設定：〈To Station〉/〈From Station〉
CWin min→AC_BK(15)
AC_BE(15)
AC_VI(7)
AC_VO(3)
〈To Station〉
CWin max→AC_BK(1023)
AC_BE(63)
AC_VI(15)
AC_VO(7)]
〈From Station〉
CWin max→AC_BK(1023)
AC_BE(1023)
AC_VI(15)
AC_VO(7)]

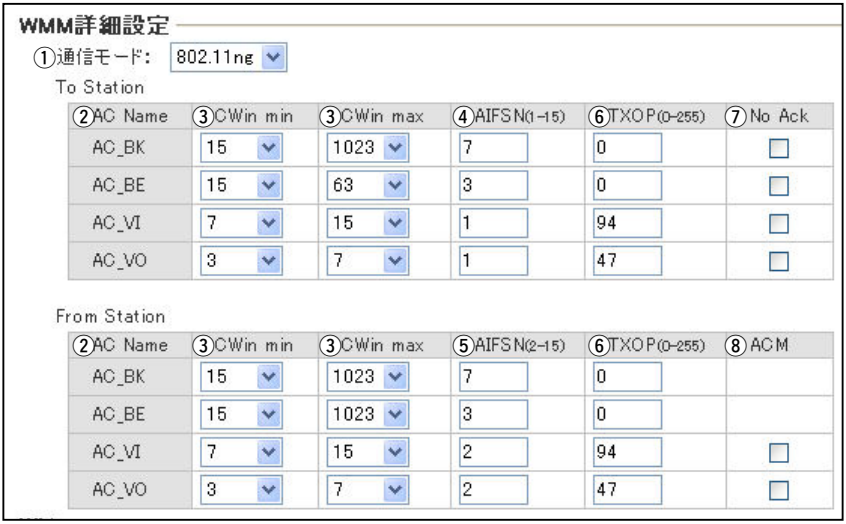
④AIFSN(1-15)：…… Arbitration Interframe Space Number(フレーム送信間隔)を設定します。
設定値が小さいほど、バックオフ制御を開始する時間が早くなるため優先度が高くなります。
設定できる範囲は、「1～15」です。

（出荷時の設定：〈To Station〉
AC_BK(7)
AC_BE(3)
AC_VI(1)
AC_VO(1)

10.「WMM詳細」画面

■ WMM詳細設定

「無線設定」ー**「WMM詳細」**


WMM詳細設定
①通信モード: 802.11ng
To Station
②AC Name ③CWin min ③CWin max ④AIFSN(1-15) ⑥TXOP(0-255) ⑦No Ack
AC_BK 15 1023 7 0
AC_BE 15 63 3 0
AC_VI 7 15 1 94
AC_VO 3 7 1 47
From Station
②AC Name ③CWin min ③CWin max ⑤AIFSN(2-15) ⑥TXOP(0-255) ⑧ACM
AC_BK 15 1023 7 0
AC_BE 15 1023 3 0
AC_VI 7 15 2 94
AC_VO 3 7 2 47

⑤**AIFSN(2-15)**：…… Arbitration Interframe Space Number(フレーム送信間隔)を設定します。
設定値が小さいほど、バックオフ制御を開始する時間が早くなるため優先度が高くなります。
設定できる範囲は、「2～15」です。

（出荷時の設定：〈From Station〉
AC_BK(7)
AC_BE(3)
AC_VI(2)
AC_VO(2)

⑥**TXOP(0-255)**： …… チャンネルアクセス権を獲得したあと、排他的にチャンネルの使用を認める期間(Transmission Opportunity)を設定します。
「0」が設定されている場合は、アクセス権獲得後に送信できるフレームは1つになります。
（出荷時の設定：〈To Station〉
AC_BK(0)
AC_BE(0)
AC_VI(94)
AC_VO(47)
〈From Station〉
AC_BK(0)
AC_BE(0)
AC_VI(94)
AC_VO(47)

⑦**No Ack**： …… ACK(受信完了通知)による再送信制御についての設定です。
再送信制御をしないときは、チェックボックスにチェックマーク[✔]を入れます。 （出荷時の設定：AC_BK □
AC_BE □
AC_VI □
AC_VO □）

⑧**ACM**： …… ACM(Admission Control Mandatory)を設定します。
ACMで保護されたカテゴリーで通信するときは、チェックボックスにチェックマーク[✔]を入れます。
（出荷時の設定：AC_VI □
AC_VO □）
※ACMで保護されたカテゴリーで通信するには、この機能に対応した無線LAN端末の設定が必要です。

10.「WMM詳細」画面

■ WMM共通設定

「無線設定」ー**「WMM詳細」**

IEEE802.11e U-APSD(Unscheduled Automatic Power Save Delivery)機能対応のFOMA®/無線LANデュアル携帯電話を省電力制御するときの設定です。

①WMMパワーセーブを使用:

…… WMMパワーセーブの使用を設定します。
（出荷時の設定:する）

※「N902iL」、「onefone™」などのNTTドコモ FOMA®/無線LANデュアル端末がWMMパワーセーブに対応しています。

※「する」に設定すると、無線LAN端末側がWMMパワーセーブ機能を使用したとき、自動的に有効になります。

②CAC通話制限台数:

…… コール・アドミッション・コントロール機能によるIP電話の最大通話数を設定します。（出荷時の設定:6）
IP電話の最大通話数を制限することで、音声通信の品質を確保できます。
設定できる範囲は、「1～63」です。

※次ページの「制限台数倍率の目安」を参考に設定してください。

※CAC設定を使用するには、[WMM詳細設定]項目から[ACM:]欄(☞P131)の設定が必要です。

※コール・アドミッション・コントロール機能に対応するNTTドコモ FOMA®/無線LANデュアル端末は、「N902iL」、「onefone™」です。

③未使用の帯域: …… 全使用帯域に対する未使用帯域の割合を表示します。

制限台数倍率の目安：[IEEE802.11g]規格の場合

CODEC / 通信速度	G711 (20ms)	G711 (40ms)	G729a (20ms)	G723.1 (30ms)	G729a (40ms)
1Mbps	1.00	1.17	2.00	2.83	3.50
2Mbps	1.67	2.17	2.83	4.17	5.33
5.5Mbps	3.00	4.50	4.17	6.00	7.83
11Mbps	3.83	6.33	4.67	6.83	9.00
6Mbps	6.00	7.50	12.50	17.83	21.67
9Mbps	8.00	10.50	15.33	21.83	27.17
12Mbps	10.33	13.83	18.83	27.33	34.00
18Mbps	13.50	18.67	22.00	31.67	40.33
24Mbps	16.17	23.17	25.00	36.33	46.33
36Mbps	19.67	29.83	27.50	40.00	51.83
48Mbps	22.00	34.83	29.00	42.17	55.17
54Mbps	22.83	36.83	29.33	42.67	56.50

通信速度を「1Mbps」、CODEC規格を「G711(20ms)」とした基準を「1」として、無線LAN端末の通信速度を変化させたときの通話制限台数に対する倍率の目安です。

【例】CAC通話制限台数が「6」（出荷時の設定）の場合、1Mbps端末では6台に制限されますが、5.5Mbpsでは18台まで収容できます。（表中：倍率3.00）

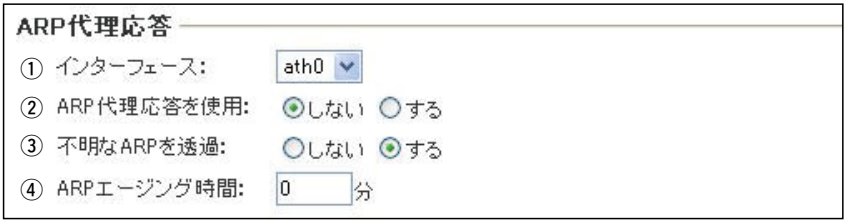
なお、通信条件などによって多少異なる場合がありますのでご注意ください。

11.「ARP代理応答」画面

■ ARP代理応答

「無線設定」ー**「ARP代理応答」**

無線LAN端末へのARPリクエストに対する応答を代理することで、無線LAN端末の省電力制御をする機能の設定です。



①インターフェース:

…… 設定する仮想AP(アクセスポイント)の名称を選択します。 (出荷時の設定:ath0)
「ath0」~「ath3」の仮想APを選択できます。
[ARPキャッシュ情報]項目(☞P136)には、選択した仮想AP(ath0~ath3)と通信する無線LAN端末の通信を常に監視し、IPv4無線LAN端末のMACアドレスとIPアドレスを表示します。

②ARP代理応答を使用:

…… [インターフェース:](①)欄で選択した仮想APについて、ARP代理応答の機能を使用するかしないかを設定します。 (出荷時の設定:しない)

③不明なARPを透過:

…… [インターフェース:](①)欄で選択した仮想APと通信している無線LAN端末すべてのARP情報がわかっていて、不明なARPが来たとき、透過するかしないかを設定します。 (出荷時の設定:する)

④ ARPエージング時間:

…… 学習したARP情報を削除するまでの時間を設定します。
（出荷時の設定:0）

※ARP情報を学習後、設定した時間が経過すると、該当するARP情報が削除されます。

※「0」（出荷時の設定）のときは、削除されません。

※無線LAN端末が無線アクセスポイント（本製品）から離脱した場合は、時間設定にかかわらずARP情報が削除されます。

【ご参考に】

ARPリクエストを受信したとき、アクセスポイントに接続している無線LAN端末のIPアドレス学習状況によって、下記のような処理をします。

◎ IPアドレス学習済みの無線LAN端末だけが存在する場合

ARPリクエストのTargetIPが学習したIPアドレスと一致する場合は、アクセスポイントが代理応答します。

一致しない場合、[不明なARPを透過:]（③）欄の設定が「する」の場合は透過、「しない」の場合は破棄します。

◎IPアドレスを学習していない無線LAN端末が1台でもいる場合

ARPリクエストのTargetIPが学習したIPアドレスと一致する場合は、アクセスポイントが代理応答します。

一致しない場合、[不明なARPを透過:]（③）欄の設定に関係なく、ARPリクエストを透過します。

11.「ARP代理応答」画面

■ ARPキャッシュ情報

「無線設定」ー**「ARP代理応答」**

学習したARP情報をMACアドレスとIPアドレスの組み合わせで表示し、必要に応じて削除するための画面です。

①**〈削除〉**…… [ARP代理応答]項目の[インターフェース:]欄(☞P134)で選択したインターフェースが学習したARPキャッシュ情報を削除するボタンです。

②**〈一括削除〉**…… [ARP代理応答]項目の[インターフェース:]欄(☞P134)で選択したインターフェースが学習したARPキャッシュ情報を一括して削除するボタンです。

12.「WPS」画面

■ WPS設定

「無線設定」ー「WPS」

WPS(Wi-Fi Protected Setup)機能の使用についての設定です。

※WPS(Wi-Fi Protected Setup)とは、無線LANの[SSID]と[暗号化方式]の設定を容易にするために、「Wi-Fiアライアンス」が提唱する機能です。

①使用するインターフェース:

…… WPS機能を使用する仮想AP(ath0～ath3)を設定します。 (出荷時の設定:なし)

※相手の無線LAN端末は、WPS機能対応の製品が必要です。

※ANY接続拒否(☞P106)との併用は、できません。

※使用できる認証方式は、「WPA-PSK ·WPA2-PSK」(☞P109)だけです。

※使用できる暗号化方式は、「TKIP ·AES」(☞P112)だけです。
また、「TKIP」の場合、[IEEE802.11n]規格で通信できません。

※自動設定する[SSID]と[PSK(Pre-Shared Key)]は、本製品側で自動生成(☞P142)、または手動(☞P52)で設定できます。

※2台目の無線LAN端末に自動設定する場合は、すでに本製品に自動設定された内容が配布されます。

12.「WPS」画面

■ WPS設定

「無線設定」ー**「WPS」**

②〈登録〉/〈取消〉/〈登録して再起動〉

…… [使用するインターフェース:]欄からインターフェース名(ath0～ath3)を選択後、この画面上で〈登録して再起動〉をクリックします。

※〈登録〉をクリックした状態では、WPS機能の〈開始〉ボタンが[WPS開始]項目(☞P139)に表示されません。〈取消〉は、「WPS」画面で〈登録〉をクリックする前に変更した内容を元に戻すときクリックします。

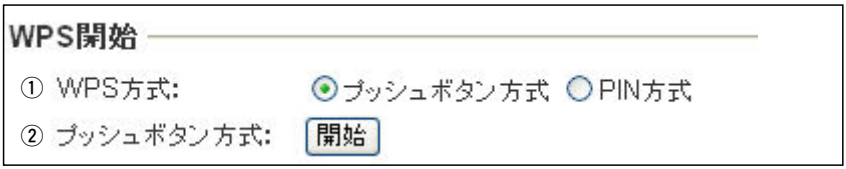
■ WPS開始

「無線設定」ー「WPS」

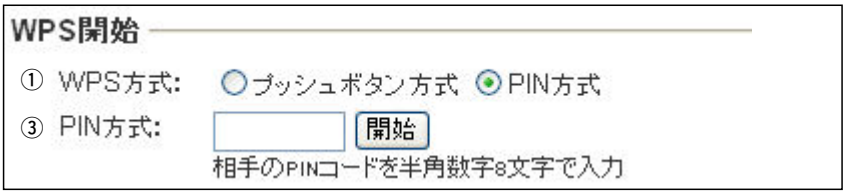
[SSID]と[暗号化方式]の自動設定を開始するための操作画面です。

※本製品の後面パネルにある〈WPS〉ボタンを使用しないで、下記の画面上から自動設定を開始するとき使用します。

◆[WPS方式:]欄で「プッシュボタン方式」をクリックしたとき



◆[WPS方式:]欄で「PIN方式」をクリックしたとき



①WPS方式: …… 自動設定の方式を選択します。

（出荷時の方式:プッシュボタン方式）

「プッシュボタン方式」:

本製品側で自動生成(☞P142)、または手動(☞P52)で設定した[SSID]と暗号化の設定を、本製品と無線LAN端末(WPS対応)のワンボタン操作で自動設定する方式です。

「PIN方式」:

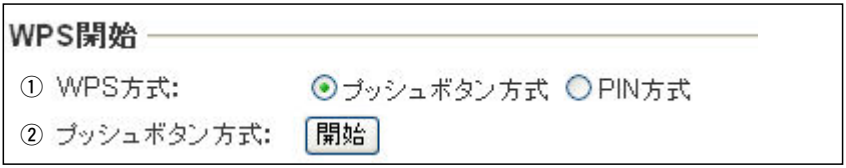
本製品側で自動生成(☞P142)、または手動(☞P52)で設定した[SSID]と暗号化の設定を、本製品に設定したPINコード(☞P141)の無線LAN端末(WPS対応)に自動設定する方式です。

※「PIN方式」で無線LAN端末側から本製品を自動設定する場合、本製品のPINコードは、142ページに記載の方法で確認できます。

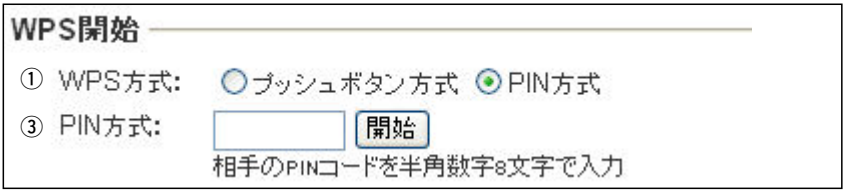
12.「WPS」画面

■ WPS開始

「無線設定」ー**「WPS」**



◆[WPS方式:]欄で「PIN方式」をクリックしたとき



②プッシュボタン方式:

…… プッシュボタン方式で自動設定を開始するための〈開始〉ボタンを表示します。
自動設定を開始するときは、表示された〈開始〉ボタンをクリックするか、本製品の後面パネルにある〈WPS〉ボタンを押します。

※〈開始〉ボタンの表示は、[WPS設定]項目の[使用するインターフェース:]欄からインターフェース名(ath0～ath3)を選択後、〈登録して再起動〉をクリックして再起動が完了するまで表示しません。

※自動設定を開始すると、本製品の[MODE]ランプが点滅(緑)します。
自動設定に成功したときは、[MODE]ランプが点灯(緑)します。

※〈開始〉ボタンを操作後、2分以内に、無線LAN端末側の自動設定操作を開始してください。
2分以上経過したり、2台以上の無線アクセスポイントや無線LAN端末が本製品に対してWPSを同時に実行したりしたとき、[MODE]ランプが点滅(赤)して、自動設定を中止しますので、本製品と無線LAN端末の操作をはじめからやりなおしてください。

③**PIN方式：** …… PIN方式で自動設定を開始するための[PINコード入力]欄〈開始〉ボタンを表示します。

※WPSに対応する無線LAN端末のPINコードは、8桁（半角数字）で入力してください。
PINコードが不明な場合は、ご使用になる無線LAN端末に付属する取扱説明書でご確認ください。

※自動設定を開始すると、本製品の[MODE]ランプが点滅（緑）します。
自動設定に成功したときは、[MODE]ランプが点灯（緑）します。

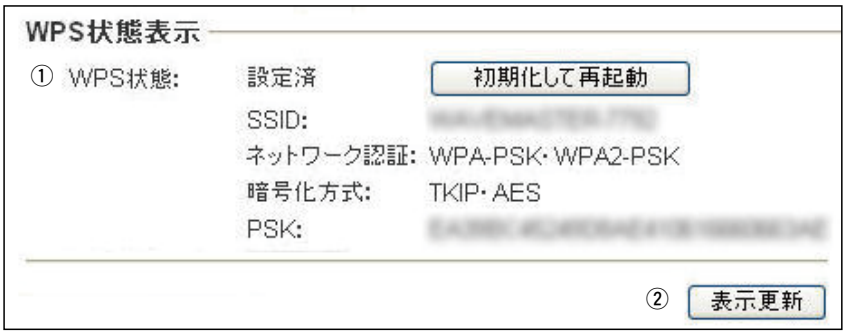
※〈開始〉ボタンを操作後、2分以内に、無線LAN端末側の自動設定操作を開始してください。
2分以上経過したり、2台以上の無線アクセスポイントや無線LAN端末が本製品に対してWPSを同時に実行したりしたとき、[MODE]ランプが点滅（赤）して、自動設定を中止しますので、本製品と無線LAN端末の操作をはじめからやりなおしてください。

12.「WPS」画面

■ WPS状態表示

「無線設定」ー**「WPS」**

WPS機能で自動設定された内容の確認と削除に使用します。



①**WPS状態:** …… WPS機能により自動設定された内容と併せて、その状態を「未設定」/「設定済」/「停止」/「初期化中」で表示します。
※自動設定された内容を削除するときは、〈初期化して再起動〉をクリックします。

②**〈表示更新〉** …… [WPS状態:](①)欄に表示する内容を更新します。

本製品のPINコードについて

本製品のPINコード(8桁の半角数字)は、WPS対応の無線LAN端末で生成した[SSID]と[暗号化方式]をPIN方式で本製品に自動設定をするときに必要になります。
必要な場合は、下記のコマンドをtelnet(☞P169)から指定すると確認できます。

▶telnetコマンド:

```
AP-80 # wireless wps enrollee start_pin
Starting WPS PIN method as Enrollee (own_pin=8      51).
```

13.「管理者」画面

■ 管理者パスワードの変更

「システム設定」ー**「管理者」**

本製品の設定画面にアクセスするためのパスワードを変更します。

①**管理者ID:** …… 本製品の設定画面にアクセスしたとき、ユーザー名の入力を求められますので、そこに[管理者ID]として、「admin」を入力します。
※本製品の[管理者ID]は、変更できません。

②**現在のパスワード:** …… 新しいパスワードに変更するとき、現在のパスワードを大文字/小文字の区別に注意して入力します。
（出荷時の設定：wavemaster）
※入力中の文字は、すべて「＊（アスタリスク）」、または「●（黒丸）」で表示します。

③**新しいパスワード:** …… 新しいパスワードを入力します。
大文字/小文字の区別に注意して、任意の英数字（半角31文字以内）で入力します。
※新しいパスワードを登録後は、設定内容がマスクされ、すぐにパスワードの入力を求める画面を表示しますので、そこに新しいパスワードを入力します。

④**新しいパスワード再入力:**
…… 確認のために、新しいパスワードを再入力します。

【ご注意】
管理者パスワードを忘れた場合、設定を確認できなくなりますのでご注意ください。
※お忘れの場合、本製品の〈MODE〉ボタンを本書160ページの操作にしたがい、設定を工場出荷時（初期化）の状態に戻していただくことになります。

14.「時計」画面

■ 自動時計設定

「システム設定」ー**「時計」**

本製品の内部時計を自動設定するとき、アクセスするタイムサーバーの設定です。

①自動時計設定を使用:

…… 本製品の自動時計設定機能を設定します。
（出荷時の設定:しない）
「する」に設定すると、インターネット上に存在するタイムサーバーに日時の問い合わせをして、内部時計を自動設定します。

②NTPサーバーIPアドレス1:

…… アクセスするタイムサーバーのIPアドレスを入力します。（出荷時の設定:210.173.160.27）
返答がないときは、[NTPサーバーIPアドレス2]（③）欄で設定したタイムサーバーにアクセスします。
※出荷時のNTPサーバーアドレスは、インターネットマルチフィード株式会社（http://www.jst.mfeed.ad.jp/）のものです。

③NTPサーバーIPアドレス2:

…… [NTPサーバー IPアドレス1:]の次にアクセスさせるタイムサーバーがあるときは、そのIPアドレスを入力します。（出荷時の設定:210.173.160.57）

④アクセス時間間隔:

…… タイムサーバーにアクセスする間隔を設定します。
設定できる範囲は、「1～99(日)」です。
(出荷時の設定:1)

※設定した日数でアクセスできなかったときは、次の間隔までアクセスしません。

※NTPサーバーにアクセスするには、経路を設定する必要があります。
経路を設定しないときは、アクセスできません。
「ネットワーク設定」メニュー→「LAN側IP」画面→[IPアドレス設定]項目にある[デフォルトゲートウェイ:]欄(☞P68)を設定してください。

⑤前回アクセス日時:

…… タイムサーバーにアクセスした日時を表示します。

⑥次回アクセス日時:

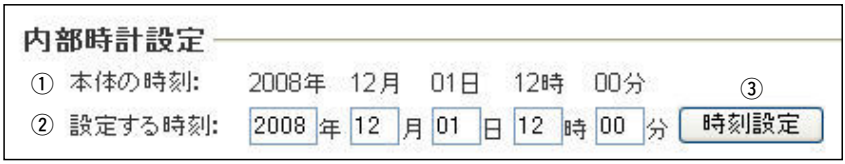
…… タイムサーバーにアクセスする予定日時を、[前回アクセス日時](⑤)欄と[アクセス時間間隔](④)欄で設定された日数より算出して表示します。

14.「時計」画面

■ 内部時計設定

「システム設定」ー**「時計」**

本製品の内部時計を設定します。



①**本体の時刻**:…… 本製品に設定されている時刻を表示します。

②**設定する時刻**:…… 本製品の設定画面にアクセスしたときの時刻を表示します。
※WWWブラウザーの〈更新〉をクリックすると、端末の時計設定を取得して表示します。

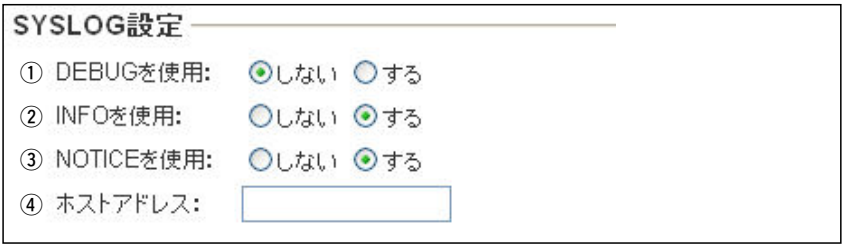
③**〈時刻設定〉**…… [設定する時刻](②)欄に表示された時刻を本製品に設定するボタンです。
※時刻を正確に設定するときは、本製品の設定画面にアクセスしなおすか、WWWブラウザーの〈更新〉をクリックしてから、〈時刻設定〉をクリックしてください。

15.「SYSLOG」画面

■ SYSLOG設定

「システム設定」ー「SYSLOG」

指定したホストにログ情報などを出力するための設定です。



①DEBUGを使用: …… 各種デバッグ情報をSYSLOGに出力する設定です。
（出荷時の設定:しない）

②INFOを使用: …… INFOタイプのメッセージをSYSLOGに出力する設定です。（出荷時の設定:する）

③NOTICEを使用: …… NOTICEタイプのメッセージをSYSLOGに出力する設定です。（出荷時の設定:する）

④ホストアドレス: …… SYSLOG機能を使用する場合、SYSLOGを受けるホストのアドレスを入力します。
※ホストは、SYSLOGサーバー機能に対応している必要があります。

16.「SNMP」画面

■ SNMP設定

「システム設定」ー「SNMP」

TCP/IPネットワークにおいて、ネットワーク上の各ホストから本製品の情報を自動的に収集してネットワーク管理するときの設定です。

①SNMPを使用:

…… 本製品のSNMP機能を設定します。

（出荷時の設定:する）

「する」に設定すると、本製品の設定情報をSNMP管理ツール側で管理できます。

②コミュニティーID(GET):

…… 本製品の設定情報をSNMP管理ツール側から読み出すことを許可するIDを、半角31文字以内の英数字で入力します。（出荷時の設定:public）

③場所: …… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される場所を、半角127文字以内の英数字で入力します。

④連絡先: …… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される連絡先を、半角127文字以内の英数字で入力します。

17.「ネットワーク情報」画面

■ インターフェースリスト

「情報表示」ー**「ネットワーク情報」**

本製品のネットワークインターフェースとそのIPアドレスについて、その詳細を表示します。

インターフェース リスト

インターフェース	IPアドレス	サブネットマスク
lo0	127.0.0.1	255.255.255.255
mirror0	192.168	255.255.255.0

■ 本体MACアドレス

「情報表示」ー**「ネットワーク情報」**

本製品のMACアドレスを表示します。

本体MACアドレス

00-90-C7-

MACアドレスは、本製品のようなネットワーク機器がそれぞれ独自に持っている機器固有の番号で、12桁(0090C7××××××)で表示されています。
また、本製品の底面パネルに貼られているシリアルシールにも、同じ内容で記載しています。

■ 無線LANユニット

「情報表示」ー**「ネットワーク情報」**

本製品で使用している仮想AP(ath0～ath3)の一覧を表示します。

無線LANユニット

インターフェース	SSID	BSSID
ath0	WAVEMASTER	00-90-C7-
ath1	WAVEMASTER	06-90-C7-
ath2	WAVEMASTER	0A-90-C7-
ath3	WAVEMASTER	0E-90-C7-

※「無線設定」メニュー→「無線LAN」画面→[無線LAN設定]項目にある[無線UNITを使用:]欄(☞P96)で「しない」を設定している場合は、上記の一覧を表示しません。

※「無線設定」メニュー→「仮想AP」画面→[仮想AP設定]項目にある[仮想APを使用:]欄(☞P105)で「しない」を設定している仮想APのインターフェースは、上記の一覧に表示しません。

18.「SYSLOG」画面

■ SYSLOG

「情報表示」ー「SYSLOG」

本製品がホストに出力するログ情報を表示します。

※上図のログ情報は表示例です。

①**表示するレベル:** …… ログ情報の各レベルについて、表示/非表示を選択します。
非表示に設定するときは、非表示にするレベルのチェックボックスをクリックして、チェックマーク[✔]をはずします。 (出荷時の設定: ☑ DEBUG ☑ INFO ☑ NOTICE)

②**〈最新状態に更新〉**…… 表示内容を最新の状態にするボタンです。

③**〈消去〉** …… 表示されたログ情報を削除するボタンです。

19.「無線LANユニット」画面

■ アクセスポイント情報

「情報表示」ー「無線設定情報一覧」ー**「無線LANユニット」**

下記(① ～ ⑤)の無線アクセスポイント情報を表示します。

①使用中チャンネル:

…… 本製品の無線通信に使用するチャンネルの設定と帯域幅モード(20MHz/40MHz)の設定(☞P97)を表示します。

②WMM ACM: …… 無線通信に使用するチャンネルについて、WMM機能のACM設定(☞P131)を表示します。

③WMMパワーセーブ:

…… 無線通信に使用するチャンネルについて、WMMパワーセーブの設定(☞P132)を表示します。

④現在時刻: …… 本製品の時刻設定(☞P146)を表示します。

⑤稼働時間: …… 本製品の稼働時間を表示します。
※電源を切る、または設定の変更や初期化に伴う再起動で、それまでの稼働時間は初期化されます。

19.「無線LANユニット」画面

■ 仮想AP一覧

「情報表示」ー「無線設定情報一覧」ー**「無線LANユニット」**

各仮想AP(ath0～ath3)の設定状況を仮想APごとに一覧で表示します。
使用していない仮想APの一覧は、インターフェース欄以外が空白になります。

仮想AP一覧

①	インターフェース	ath0
②	SSID	WAVEMASTER-0
③	VLAN ID	0
④	ANY接続拒否	使用しない
⑤	暗号化	なし
⑥	MACアドレスフィルタリング	使用しない
⑦	ARP代理応答	使用しない

※「ath0」の一覧を例に説明しています。

①インターフェース
…… 仮想APの名称(ath0～ath3)を表示します。

②SSID …… 仮想AP(例:ath0)に設定された[SSID](☞P105)を表示します。

③VLAN ID …… 仮想AP(例:ath0)に設定された[VLAN ID](☞P106)を表示します。

④ANY接続拒否 …… 仮想AP(例:ath0)に対する[ANY接続拒否](☞P106)の使用状況を表示します。

⑤暗号化 …… 仮想AP(例:ath0)に設定された[ネットワーク認証](☞P108、P109)と[暗号化方式](☞P110～P112)を表示します。
設定されていないときは、「なし」を表示します。

⑥MACアドレスフィルタリング
…… 仮想AP(例:ath0)に対する[MACアドレスフィルタリング](☞P120、P121)の使用状況を表示します。

⑦ARP代理応答 …… 仮想AP(例:ath0)に対する[ARP代理応答](☞P134)の使用状況を表示します。

20.「端末情報」画面

■ 端末情報

「情報表示」ー「無線設定情報一覧」ー**「端末情報」**

本製品の仮想AP(ath0～ath3)と通信する無線LAN端末があるとき、その無線LAN端末との通信情報を表示します。

※上図は、無線LAN端末と通信時の表示例です。

①**〈最新状態に更新〉**…… 表示内容を最新の状態にするボタンです。

②**帰属AP** …… 無線LAN端末との通信に使用する仮想APの名称(例:ath0)を表示します。

③**MACアドレス** …… 本製品と通信する無線LAN端末のMACアドレスを表示します。

④**IPアドレス** …… 本製品と通信する無線LAN端末のIPアドレスを表示します。

⑤**通信モード** …… 無線LAN端末との通信に使用する無線LAN規格を表示します。

◎802.11naを表示する場合
[IEEE802.11n/a(W52/W53/W56)]規格で無線通信しているとき

◎802.11a表示する場合
[IEEE802.11a(W52/W53/W56)]規格で無線通信しているとき

◎802.11ngを表示する場合
[IEEE802.11n/g]規格で無線通信しているとき

◎802.11bgを表示する場合
[IEEE802.11b/g]規格で無線通信しているとき

⑥**〈詳細〉** …… 通信中の無線LAN端末の「無線通信詳細情報」を別画面(☞P154)で表示します。

20.「端末情報」画面

■ 通信端末詳細情報

「情報表示」ー「無線設定情報一覧」ー**「端末情報」**

本製品と通信するの無線LAN端末ごとの詳細情報を表示します。

※「MACアドレスフィルタリング」画面の［無線通信状態］（☞P125、P126）で表示される内容も含まれています。

※上図は、無線LAN端末と通信中、「端末情報」画面（☞P153）に表示された〈詳細〉ボタンをクリックすると表示します。

①**通信状況**：…… 「未接続」/「通信中」/「認証中」/「認証失敗」など、接続状況を表示します。
※「通信不可」を表示する場合は、お買い上げの販売店、または弊社サポートセンターにお問い合わせください。

②**MACアドレス**：…… 無線LAN端末のMACアドレスを表示します。

③**IPアドレス**：…… 無線LAN端末のIPアドレスを表示します。

④**通信モード**：…… 無線LAN端末との通信に使用する無線LAN規格を表示します。
◎802.11naを表示する場合
［IEEE802.11n/a(W52/W53/W56)］規格で無線通信しているとき
◎802.11a表示する場合
［IEEE802.11a(W52/W53/W56)］規格で無線通信しているとき
◎802.11ngを表示する場合
［IEEE802.11n/g］規格で無線通信しているとき
◎802.11bgを表示する場合
［IEEE802.11b/g］規格で無線通信しているとき

⑤**SSID**：…… 無線LAN端末のSSIDを表示します。

⑥**暗号化**：…… 無線LAN端末との通信に使用している認証モード･暗号化方式を表示します。

⑦**チャンネル**：…… 無線LAN端末との通信に使用しているチャンネルを表示します。

⑧**信号レベル**：…… 無線LAN端末から受信した電波信号の強さを、メーターと数値で表示します。
安定した通信の目安は、「緑(15)」以上のレベルです。

表　示	［赤］	［黄］	［緑］	［青］
レベル	0～4	5～14	15～29	30以上

⑨**速度**：…… 本製品の通信速度を理論値(Mbps)で表示します。

⑩**WMM**：…… 無線通信に使用するチャンネルについて、WMM機能の使用状況を表示します。

20.「端末情報」画面

■ 通信端末詳細情報

「情報表示」ー「無線設定情報一覧」ー**「端末情報」**

※上図は、無線LAN端末と通信中、「端末情報」画面(☞P153)に表示された〈詳細〉ボタンをクリックすると表示します。

⑪WMMパワーセーブ:
…… 無線通信に使用するチャンネルについて、WMMパワーセーブの使用状況を表示します。

⑫WMM CAC使用率:
…… 全使用帯域に対する使用帯域の割合を表示します。

⑬接続時間: …… 無線LAN端末と無線通信した(無通信状態を除く)時間を表示します。
※4分～5分以上、無線通信しない(無通信)状態がつづいたときは、再度アクセスしなおしたときからの通信時間が表示されます。

保守について

第6章

この章では、
本製品の設定内容保存や初期化、ファームウェアのバージョンアップをする手順について説明しています。

1. 設定内容の確認または保存 …… 158
　確認と保存のしかた …… 158
2. 保存された設定の書き込み …… 159
　書き込みかた …… 159
3. 設定を出荷時の状態に戻すには …… 160
　Ⓐ〈MODE〉ボタンを使用する …… 160
　Ⓑ 設定画面を使用する …… 161
4. ファームウェアをバージョンアップする …… 162
　ファームウェアについて …… 162
　ファイルを指定して更新する …… 163

6 保守について

1. 設定内容の確認または保存

本製品の設定画面で変更された内容を確認したり、その内容を設定ファイルとしてパソコンに保存したりできます。

※設定を保存しておくと、誤って設定内容が失われたときなどに利用できます。

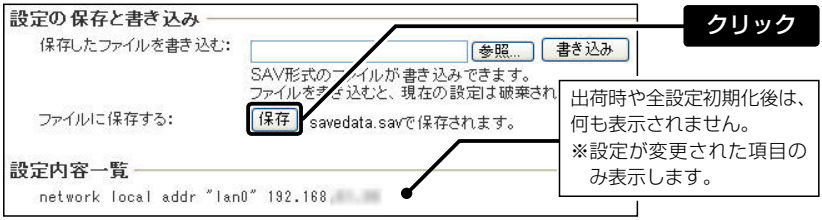
確認と保存のしかた

「メンテナンス」→**「設定保存」**

1 本製品の設定画面にアクセスします。(☞P37)

2 「メンテナンス」メニューをクリックします。
「設定保存」画面を表示します。

3 [ファイルに保存する]欄の〈保存〉をクリックします。
「ファイルのダウンロード」画面(別画面)を表示します。



4 「ファイルのダウンロード」画面の〈保存(S)〉をクリックします。
「名前を付けて保存」画面(別画面)を表示します。

5 保存する場所に変更がない場合は、〈保存(S)〉をクリックします。
「.sav」の拡張子がついた設定ファイルが、選択した場所に保存されます。

2. 保存された設定の書き込み

保存した設定ファイル(☞P158)を本製品に書き込む手順を説明します。

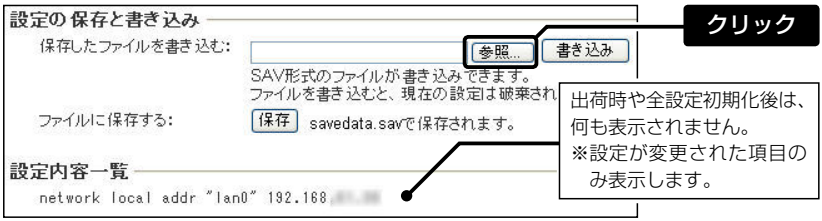
書き込みかた

「メンテナンス」→**「設定保存」**

1 本製品の設定画面にアクセスします。(☞P37)

2 「メンテナンス」メニューをクリックします。
「設定保存」画面を表示します。

3 設定ファイルの保存先を指定するため、〈参照...〉をクリックします。
「ファイルの選択」画面(別画面)を表示します。



4 「ファイルの選択」画面から保存された設定ファイルを指定して、〈開く(O)〉をクリックします。
[保存したファイルを書き込む:]欄のテキストボックスに、保存先が表示されます。

5 [設定の保存と書き込み]項目(☞手順3.)で、〈書き込み〉をクリックします。
「設定データを復元しています」が表示され、設定ファイルの内容を本製品に書き込みます。

6 書き込み後、開いている設定画面を閉じて、設定画面にアクセスしなおします。
現在開いている画面の状態では、書き込まれた設定が反映されません。

【ご注意】

本製品の設定ファイルを本製品以外の機種に書き込まないでください。
本製品の設定ファイルを本製品以外の機器に組み込んだり、改変や分解したりしたことによる障害、および本製品の故障、誤動作、不具合、破損、データの消失あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益または第三者からのいかなる請求についても当社は一切その責任を負いかねますので、あらかじめご了承ください。

3. 設定を出荷時の状態に戻すには

ネットワーク構成を変更するときなど、既存の設定データをすべて消去して、設定をはじめからやりなおすときは、本製品の設定内容を出荷時の状態に戻せます。
そのときの状況に応じて、次の2とおりの方法があります。

Ⓐ〈MODE〉ボタンを使用する
※本製品に設定されたIPアドレスが不明な場合など、設定画面にアクセスできないとき

Ⓑ 設定画面を使用する(☞P161)

Ⓐ〈MODE〉ボタンを使用する

初期化すると、すべての設定項目が出荷時の状態になります。

パソコンに設定されたIPアドレスのネットワーク部が本製品(出荷時の設定:192.168.0.1)と異なると、設定画面にアクセスできなくなりますので、必要に応じてパソコンのIPアドレスを変更してください。

1 本製品からすべてのネットワーク機器を取りはずして、電源を接続します。

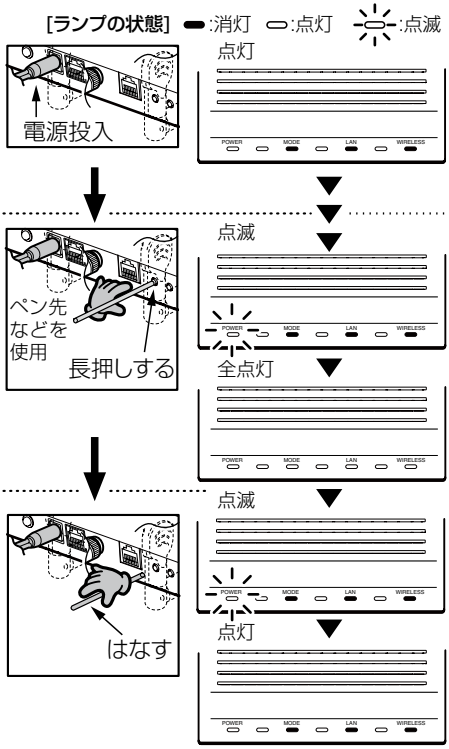
[POWER]ランプだけが点灯します。

2 〈MODE〉ボタンを長く(5秒以上)押します。

[POWER]ランプが点滅を繰り返します。
※[POWER]ランプが点灯してから操作を開始してください。

3 すべてのランプが同時点灯に切り替わったとき、〈MODE〉ボタンから手をはなします。

[POWER]ランプが数回点滅したあと、点灯に切り替わるまで待つと、初期化完了です。



本製品に設定されたIPアドレスがわかっていて、そのIPアドレスで設定画面にアクセスできるときは、本製品の設定画面から、すべての設定を出荷時の状態に戻せます。

Ⓑ 設定画面を使用する

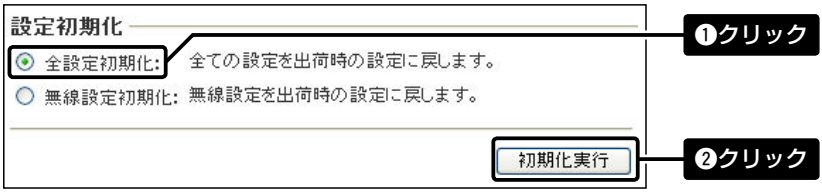
「メンテナンス」→**「設定初期化」**

IPアドレスが不明な場合などの初期化については、本書160ページをご覧ください。

1 本製品の設定画面にアクセスします。(☞P37)

2 「メンテナンス」メニュー、[設定初期化]の順にクリックします。
「設定初期化」画面を表示します。

3 初期化したい条件をクリックして、〈初期化実行〉をクリックします。
クリックした条件に該当する設定内容が出荷時の設定に戻ります。



4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。
[ユーザー名(U):]と[パスワード(P):]を求める画面が表示されます。(☞P37)

6

初期化の条件について

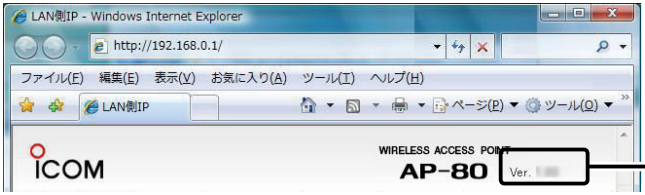
- **全設定初期化を選択した場合**
  本製品に設定されたすべての内容を出荷時の状態に戻します。
  初期化実行後は、「192.168.0.1(出荷時の設定)」で動作します。
  初期化によって、パソコンに設定されたIPアドレスのネットワーク部が本製品と異なったときは、アクセスできなくなりますので、必要に応じてパソコンのIPアドレスを変更してください。(☞2章)
- **無線設定初期化を選択した場合**
  「無線設定」メニューで設定した内容だけを出荷時の状態に戻します。
  初期化実行後は、「wavemaster-0(出荷時の設定)」のSSID、暗号化されない状態で動作します。
  初期化によって、パソコンに設定されたSSIDや暗号化設定が本製品と異なったときは、アクセスできなくなりますので、必要に応じてパソコンの無線LAN設定を変更してください。(☞2章)

4. ファームウェアをバージョンアップする

本製品の設定画面からバージョンアップ(更新)できます。

ファームウェアについて

ファームウェアは、本製品を動作させるために、出荷時から本製品のフラッシュメモリーに書き込まれているプログラムです。
このプログラムは、機能の拡張や改良のため、バージョンアップをすることがあります。
バージョンアップの作業をする前に、本製品の設定画面にアクセスして、次のフレーム内に表示するバージョン情報を確認してください。
バージョンアップをすると、機能の拡張や改良により、本製品を最良の状態にできます。



バージョンアップについてのご注意

◎ファームウェアの更新中は、絶対に本体の電源を切らないでください。
途中で電源を切ると、データの消失や誤動作の原因になります。
できるだけ、有線LAN端末からのバージョンアップをおすすめします。
◎ご使用のパソコンでファイアウォール機能が動作していると、バージョンアップできないことがあります。
バージョンアップできない場合は、ファイアウォール機能を「無効」にしてください。

◆記載する操作の結果については、自己責任の範囲となりますので、次のことを守って作業をはじめてください。
弊社ホームページ(http://www.icom.co.jp/)より提供される本製品のアップデート用ファームウェアファイルを、本製品以外の機器に組み込み、改変や分解したことによる障害、および本製品の故障、誤動作、不具合、破損、データの消失あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益、または第三者からのいかなる請求についても当社は一切その責任を負いかねますのであらかじめご了承ください。

ファイルを指定して更新する

「メンテナンス」→「ファームウェアの更新」

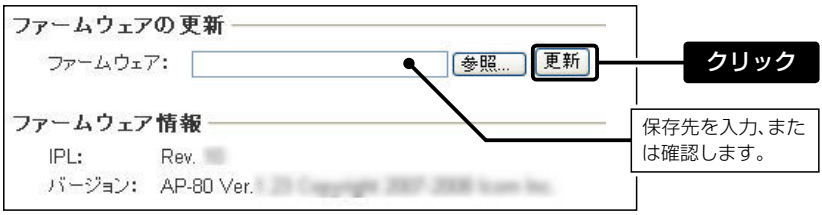
バージョンアップの前に、現在の設定ファイルの保存をおすすめします。(☞P158)

※バージョンアップ後、既存の設定内容が初期化されるファームウェアファイルがありますので、ダウンロードするときは、弊社ホームページに記載の内容をご確認ください。

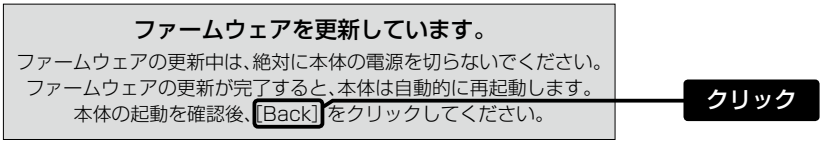
1 本製品の設定画面にアクセスします。(☞P37)

2 「メンテナンス」メニュー、[ファームウェアの更新]の順にクリックします。
「ファームウェアの更新」画面を表示します。

3 〈参照...〉をクリックして、弊社ホームページよりダウンロードしたファームウェアファイル(拡張子:dat)の保存先を指定してから、〈更新〉をクリックします。



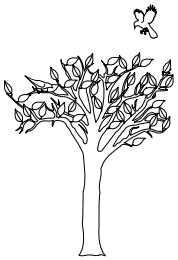
4 更新完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックすると、設定画面に戻ります。



設定画面に戻らないときは、ファームウェアファイルの更新中ですので、しばらくしてから再度クリックしてください。(接続するパソコンや本製品の電源は、絶対に切らないでください。)

【ご注意】

[Back]の操作(☞手順4.)で、設定画面に戻るまで、ご使用のパソコンや本製品の電源を絶対に切らないでください。
途中で電源を切ると、データの消失や故障の原因になります。
※出荷時の設定内容に戻るような注意書きがあるバージョンアップ用ファームウェアの場合は、[Back]をクリックしても設定画面に戻れませんので、接続するパソコンのIPアドレスを「例:192.168.0.10」に設定してから、本製品の設定画面にアクセスしなおしてください。



ご参考に

第7章

この章では、
困ったときの対処法、設定画面の構成、設定項目の初期値、仕様などを説明しています。

1. 困ったときは …… 166
2. Telnetで接続するには …… 169
   Windows XP/2000の場合 …… 169
   Windows 98/98 SE/Meの場合 …… 169
   [CONSOLE]ポートを使用する …… 170
   Telnetコマンドについて …… 171
3. 設定項目の初期値一覧 …… 172
4. 設定画面の構成について …… 174
5. PoEによる電源供給について …… 176
6. 対応無線LAN製品について …… 177
7. 暗号化対応表 …… 178

7 ご参考に

1. 困ったときは

下記のような現象は、故障でないことがありますので、修理を依頼される前にもう一度お調べください。

[POWER]ランプが点灯しない

● **ACアダプターが本製品に接続されていない**
→ ACアダプターおよびDCプラグの接続を確認する

● **ACアダプターをパソコンなどの電源と連動したコンセントに接続している**
→ 本製品のACアダプターを壁などのコンセントに直接接続する

[LAN]ランプが点灯しない

● **LANケーブルが本製品と正しく接続されていない**
→ 本製品やパソコンの[LAN]ポート、またはLANケーブルを確認する

● **パソコン、またはHUBの電源が入っていない**
→ パソコンとHUBの電源が入っていることを確認する

本製品の設定画面にアクセスできない

● **パソコンのIPアドレスを設定していない**
→ 本製品の出荷時や全設定初期化時は、パソコンのIPアドレスを固定IPアドレスに設定する(☞P26～P29)

● **IPアドレスのネットワーク部が、本製品とパソコンで異なっている**
→ パソコンに設定されたIPアドレスのネットワーク部を本製品(☞P38)と同じにする

● **無線LAN設定が、本製品とパソコンで異なっている**
→ パソコンに設定されたネットワーク認証や暗号鍵(キー)を本製品と同じにする

● **ご使用のWWWブラウザーにプロキシサーバーが設定されている**
→ Internet Explorerの「ツール」メニューから「インターネットオプション(O)...」、[接続]タブ、〈LANの設定(L)...〉ボタンの順に操作して、[設定を自動検出する(A)]や[LANにプロキシサーバーを使用する(X)]にチェックマークが入っていないことを確認する

本製品の設定画面が正しく表示しない

● **WWWブラウザーのJavaScript機能、およびCookieを無効に設定している**
→ JavaScript機能、およびCookieを有効に設定する(☞P37)

● **Microsoft Internet Explorer6.0以降を使用していない**
→ Microsoft Internet Explorer6.0以降を使用する(☞P37)

[WIRELESS]ランプが点灯しない

● パソコンの無線LANが機能していない
→ ご使用のパソコン、または無線LANアダプターに付属の取扱説明書を確認する

● 無線LAN端末と本製品の無線LAN規格が異なっている
→ ご使用になる無線LAN端末が準拠している無線LAN規格を確認する

● [IEEE802.11a]規格だけの通信に設定した無線LAN端末を使用している
→ 本製品の無線チャンネルを[IEEE802.11a(W52/W53/W56)]規格(5.2/5.3/5.6GHz帯)のチャンネルに変更する(→P46)

● 本製品の無線LAN機能を無効に設定している
→ 本製品の無線LAN機能を有効に設定する(☞P96)

● 通信終了後、無線通信しない状態が4分以上つづいた
→ 本製品に再度アクセスして点灯することを確認する

● パソコンを起動したあとで、本製品の電源を入れた
→ 本製品の電源を入れた状態で、パソコンを再起動する

● 無線LAN端末の通信モードが「アドホック」になっている
→ 無線通信モードを「インフラストラクチャー」に変更する

● SSID(またはESSID)の設定が異なっている
→ 本製品と無線LAN端末のSSIDを確認する

● 暗号化認証モードが異なるタイプである
→ 無線LAN端末、または本製品の認証モードを同じ設定にする

● MACアドレスフィルタリングを使用している
→ 無線LAN端末のMACアドレスを本製品に登録する

● 本製品のANY拒否機能を有効に設定している
→ 本製品のANY拒否機能を無効に設定する

[WIRELESS]ランプが点灯しているが通信できない

暗号化セキュリティーの設定が異なっている
→ 本製品と無線LAN端末の暗号化セキュリティーの設定を確認する

7 ご参考に

1. 困ったときは

〈WPS〉ボタンが機能しない(無線LANを自動設定できない)

● 本製品のWPS機能を無効に設定している
→ WPS機能を使用するインターフェース(ath0～ath3)を設定していないか、インターフェースの番号を間違えて設定している(☞P41)

● 無線LAN端末が無線LANの自動設定に対応していない
→ WPS対応の弊社製無線LAN端末(例:SU-80、SE-80、SE-80M)を用意する(☞P25)

● ほかの無線LAN端末と自動設定中である
→ ほかの無線LAN端末との自動設定が完了するまで待つ

● 本製品と無線LAN端末の自動設定操作を2分以内に開始できなかった
→ 自動設定操作を2分以内に開始する

● 何度繰り返しても、自動設定できない
→ WPS機能を無効に変更して、手動で設定する(☞P39、P40)

[IEEE802.11n]規格で通信できない

● 無線LAN端末が[IEEE802.11n]規格に準拠していない
→ [IEEE802.11n]規格に準拠した無線LAN端末を使用する

● 「AES」以外の暗号化セキュリティーを使用している
→ 暗号化方式を「AES」に設定する(☞P40、P112)

2. Telnetで接続するには

Telnetでの接続について説明します。
ご使用のOSやTelnetクライアントが異なるときは、それぞれの使用方法をご確認ください。

Windows XP/2000の場合

① Windowsを起動します。
② [スタート]メニューから[ファイル名を指定して実行]を選択します。
名前欄に「Telnet.exe」と入力し、〈OK〉をクリックします。
③ Telnetクライアントが起動しますので、下記のように指定します。
Microsoft Telnet>open 本製品のIPアドレス(出荷時の設定:192.168.0.1)
④ [login]と[Password]が要求されます。
[管理者ID(admin)]と、本製品の「管理者」画面で設定した[管理者パスワード](出荷時の設定:wavemaster)を入力して、[Enter]キーを押してください。
⑤ ログインメッセージ(AP-80 #)が表示されます。

Windows 98/98 SE/Meの場合

① Windowsを起動します。
② [スタート]メニューから[ファイル名を指定して実行]を選択します。
名前欄に「Telnet.exe」と入力し、〈OK〉をクリックします。
③ Telnetクライアントが起動しますので、メニューバーから[接続]→[リモートシステム]を選択します。
④ [接続]ダイアログボックスが表示されます。
ホスト名、ポート、ターミナルの種類を下記のように選択して、〈接続(C)〉をクリックします。
ホスト名　　:本製品のIPアドレス(出荷時の設定:192.168.0.1)
ポート　　:telnet(23)
ターミナルの種類　:vt100
⑤ [login]と[Password]が要求されます。
[管理者ID(admin)]と、本製品の「管理者」画面で設定した[管理者パスワード](出荷時の設定:wavemaster)を入力して、[Enter]キーを押してください。
⑥ ログインメッセージ(AP-80 #)が表示されます。

Windows Vistaをご使用の場合は

「コントロールパネル」→「プログラム」→「Windows の機能の有効化または無効化」から、[Telnetクライアント]を有効にすると、上記の「Windows XP/2000の場合」と同じ手順で使用できます。

2. Telnetで接続するには

[CONSOLE]ポートを使用する

本製品の[CONSOLE]ポートとパソコンの[COM]ポートを設定用ケーブル(別売品:OPC-1402)で接続すると、ターミナルソフトから設定できます。
使用するときは、パソコンの[COM]ポートを下記の値に設定します。

◎**[接続方法]の選択**：設定用ケーブルを接続している[COM]ポートの番号を指定します。
◎**通信速度**　：115200(ビット/秒)
◎**データビット**　：8
◎**パリティ**　：なし
◎**ストップビット**　：1
◎**フロー制御**　：なし

※設定後、何も入力せずに[Enter]キーを押すと、「AP-80 #」と表示されます。

Telnetコマンドについて

本製品で使用できるTelnetコマンドの表示方法と、コマンド入力について説明します。

◎ コマンド一覧 ……[Tab]キーを押すと、使用できるコマンドの一覧が表示されます。
コマンド名の入力につづいて[Tab]キーを押すと、サブコマンドの一覧が表示されます。

◎ コマンド名の補完 ……コマンド名を先頭から数文字入力し[Tab]キーを押すと、コマンド名が補完されます。
入力した文字につづくコマンドが1つしかないときは、コマンド名を最後まで補完します。
例）s[Tab]→save
複数のコマンドがあるときは、コマンドの候補を表示します。
例）res[Tab]→reset restart

3. 設定項目の初期値一覧

本製品の設定画面について、全設定を初期化したとき表示される各項目の初期値です。

ネットワーク設定

「LAN側IP」画面
本体名称
本体名称：AP-80
VLAN設定
マネージメントID：0
IPアドレス設定
IPアドレス：192.168.0.1
サブネットマスク：255.255.255.0
デフォルトゲートウェイ：空白（設定なし）

「DHCPサーバー」画面
DHCPサーバー設定
DHCPサーバー機能を使用：しない
割り当て開始IPアドレス：192.168.0.10
割り当て個数：30（個）
サブネットマスク：255.255.255.0
リース期間：72（時間）
ドメイン名：空白（設定なし）
デフォルトゲートウェイ：空白（設定なし）
プライマリーDNSサーバー：空白（設定なし）
セカンダリーDNSサーバー：空白（設定なし）
プライマリーWINSサーバー：空白（設定なし）
セカンダリーWINSサーバー：空白（設定なし）
静的DHCPサーバー設定
MACアドレス：空白（設定なし）
IPアドレス：空白（設定なし）

「ルーティング」画面
スタティックルーティング設定
宛先：空白（設定なし）
サブネットマスク：空白（設定なし）
ゲートウェイ：空白（設定なし）

「パケットフィルター」画面
パケットフィルター（設定なし）

無線設定

「無線LAN」画面
無線LAN設定
無線UNITを使用：する
チャンネル：001CH（2412MHz）
40MHz帯域幅モード：□（✔なし〈OFF〉）
パワーレベル：高
DTIM間隔：1
プロテクション機能：有効

「仮想AP」画面（ath0～ath3）
仮想AP設定
インターフェース：ath0
仮想APを使用：する（ath0）
しない（ath1～ath3）
SSID：WAVEMASTER-0（ath0）
WAVEMASTER-1（ath1）
WAVEMASTER-2（ath2）
WAVEMASTER-3（ath3）
VLAN ID：0（ath0～ath3）
ANY接続拒否：しない（ath0～ath3）
接続端末制限：63（ath0～ath3）
アカウンティングを使用：しない（ath0～ath3）
暗号化設定
ネットワーク認証：オープンシステム・共有キー
（ath0～ath3）
暗号化方式：なし（ath0～ath3）
※ネットワーク認証の設定に応じて表示される設定項目の初期値については、本書5章をご覧ください。

「認証サーバー」画面
RADIUS設定（プライマリー／セカンダリー）
アドレス：空白（設定なし）
ポート：1812
シークレット：空白（設定なし）
アカウンティング設定
アドレス：空白（設定なし）
ポート：1813（プライマリー／セカンダリー）
シークレット：空白（設定なし）

無線設定(つづき)

「MACアドレスフィルタリング」画面(ath0～ath3)

MACアドレスフィルタリング設定
インターフェース:ath0
MACアドレスフィルタリングを使用:しない
フィルタリングポリシー:許可リスト

端末MACアドレスリスト
MACアドレス:空白(設定なし)

「WMM詳細」画面

WMM詳細設定
〈To Station〉/〈From Station〉
CWin min:AC_BK(15)、AC_BE(15)
AC_VI(7)、AC_VO(3)
〈To Station〉
CWin max:AC_BK(1023)、AC_BE(63)
AC_VI(15)、AC_VO(7)
〈From Station〉
CWin max:AC_BK(1023)、AC_BE(1023)
AC_VI(15)、AC_VO(7)
〈To Station〉
AIFSN(1-15):AC_BK(7)、AC_BE(3)
AC_VI(1)、AC_VO(1)
〈From Station〉
AIFSN(2-15):AC_BK(7)、AC_BE(3)
AC_VI(2)、AC_VO(2)
〈To Station〉/〈From Station〉
TXOP(0-255):AC_BK(0)、AC_BE(0)
AC_VI(94)、AC_VO(47)
〈To Station〉(✔なし〈OFF〉)
No Ack:AC_BK □、AC_BE □
AC_VI □、AC_VO □
〈From Station〉(✔なし〈OFF〉)
ACM:AC_VI □、AC_VO □

WMMパワーセーブ設定
WMMパワーセーブを使用:する

CAC設定
通話制限台数:6

「ARP代理応答」画面(ath0～ath3)

ARP代理応答
インターフェース:ath0
ARP代理応答を使用:しない
不明なARPを透過:する
ARPエージング時間:0(分)

無線設定(WPS)

「WPS」画面(ath0～ath3)

WPS設定
使用するインターフェース:なし

システム設定

「管理者」画面

管理者パスワードの変更
管理者ID:admin(変更不可)
現在のパスワード:wavemaster(非表示)
新しいパスワード:空白(設定なし)
新しいパスワード再入力:空白(設定なし)

「時計」画面

自動時計設定
自動時計設定を使用:しない
NTPサーバー IPアドレス1:210.173.160.27
NTPサーバー IPアドレス2:210.173.160.57
アクセス時間間隔:1(日)
※初期に参照しているNTPサーバーは、インターネットマルチフィード株式会社のものです。
http://www.jst.mfeed.ad.jp/

内部時計設定
設定する時刻:パソコンから取得した時刻

「SYSLOG」画面

SYSLOG設定
DEBUGを使用:しない
INFOを使用:する
NOTICEを使用:する
ホストアドレス:空白(設定なし)

「SNMP」画面

SNMP設定
SNMPを使用:する
コミュニティーID(GET):public
場所:空白(設定なし)
連絡先:空白(設定なし)

情報表示

「SYSLOG」画面

SYSLOG(✔あり〈ON〉)
表示するレベル:☑ DEBUG/☑ INFO/
☑ NOTICE

4. 設定画面の構成について

本製品の全設定を初期化したとき、WWWブラウザーに表示される画面構成です。

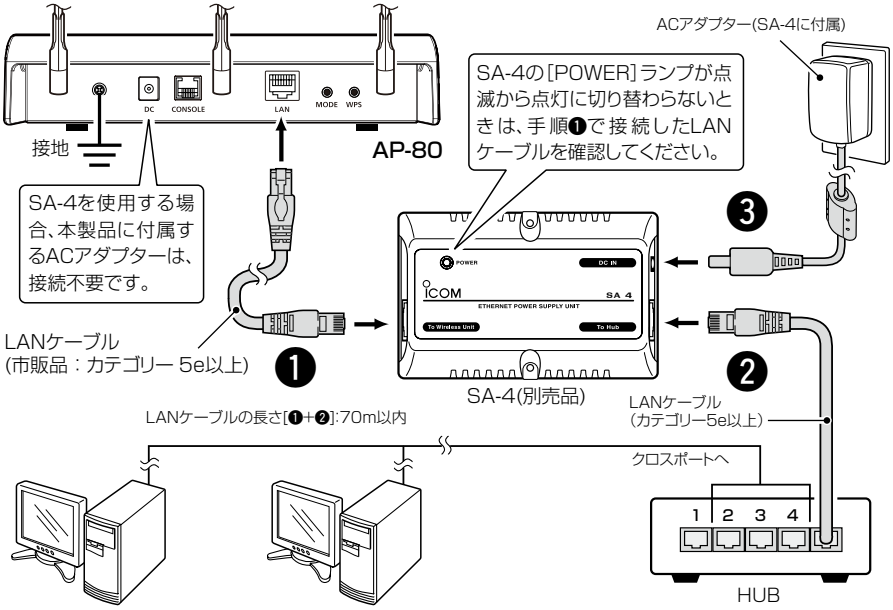
設定メニュー	設定画面	設定項目
ネットワーク設定	LAN側IP	本体名称
		VLAN設定
		IPアドレス設定
	DHCPサーバー	DHCPサーバー設定
		静的DHCPサーバー設定
		現在の登録
	ルーティング	IP経路情報
		スタティックルーティング設定
		現在の登録
	パケットフィルター	パケットフィルター
		現在の登録
無線設定	無線LAN	無線LAN設定
	仮想AP	仮想AP設定
		暗号化設定
	認証サーバー	RADIUS設定
		アカウンティング設定
	MACアドレスフィルタリング	MACアドレスフィルタリング設定
		端末MACアドレスリスト
		現在の登録
	WMM詳細	WMM詳細設定
		WMM共通設定
	ARP代理応答	ARP代理応答
		ARPキャッシュ情報
	WPS	WPS設定
		WPS開始
		WPS状態表示
システム設定	管理者	管理者パスワードの変更
	時計	自動時計設定
		内部時計設定
	SYSLOG	SYSLOG設定
	SNMP	SNMP設定

設定メニュー(つづき)	設定画面	設定項目
情報表示	ネットワーク情報	インターフェース リスト
		本体MACアドレス
		無線LANユニット
	SYSLOG	SYSLOG
無線設定情報一覧▶	無線LANユニット	アクセスポイント情報
		仮想AP一覧
	端末情報	端末情報
メンテナンス	設定保存	設定の保存と書き込み
		設定内容一覧
	設定初期化	設定初期化
	再起動	再起動
	ファームウェアの更新	ファームウェアの更新
		ファームウェア情報

5. PoEによる電源供給について

AP-80の[LAN]ポートに接続されたLANケーブルとSA-4(別売品)を接続して、本製品に電源を供給する接続方法について説明します。

※下記の図に示す番号の順に接続後、SA-4の[POWER]ランプが点滅から点灯状態に切り替わらないときは、手順❶で接続したLANケーブルを確認してください。



設置と接続のご注意

◎1台のSA-4で電源供給できるのは、本製品1台だけです。
◎AP-80に付属のACアダプターは必要ありません。
◎SA-4には、電源が必要ですので、コンセントから近い場所に設置してください。
◎HUBなどのネットワーク機器に搭載のリピーター機能は、搭載していません。
したがって、使用するLANケーブルは、HUB(HUBを使用しない場合は、パソコン)からSA-4を介して接続された本製品までの総延長距離が70m以内の場所に設置してください。
※ご使用のLANケーブルによっては、Ethernet規格の最大長制限より短くなることがあります。
◎SA-4は、防水構造ではありませんので、雨水などでぬれやすい場所には設置できません。
◎[1000BASE-T]規格でご使用になる場合、決められた規則にしたがってすべてのピンが結線されたカテゴリー5e以上のLANケーブルをご使用ください。
◎LANケーブルを接続後、SA-4のACアダプターを接続してから、SA-4の[POWER]ランプが点灯に切り替わる(起動する)まで、10秒～15秒かかることがあります。

6. 対応無線LAN製品について

本製品と無線で通信するときパソコンに装着する無線LANカードやWIRELESS LAN UNITは、下記の弊社製品がご使用いただけます。　（2009年11月現在）

◎[IEEE802.11n★1/a(W52/W53/W56)/b/g]規格準拠製品
SE-80(WPS機能対応)、SE-80M(WPS機能対応)、SU-80(WPS機能対応)
★1.[IEEE802.11n]規格は、暗号化方式を「なし」または「AES」に設定している場合に有効です。

◎[IEEE802.11a(W52/W53/W56)/b/g]規格準拠製品
SE-56W

◎[IEEE802.11a(W52/W53)/b/g]規格準拠製品
SL-5200W、SL-5300W、SE-50W、SU-50W

◎[IEEE802.11a(W52)/b/g]規格準拠製品
SL-5000XG★2、SL-5100★2、SL-5200★2、SE-50★2
★2.[IEEE802.11a(W52)]規格でご利用になる場合には、新チャンネルへの移行アップグレードが必要です。

◎[IEEE802.11b]規格準拠製品
SL-11、SL-12、SL-110、SL-120、SL-5000、SU-12

※[IEEE802.11a(J52)]規格の無線LAN端末とは通信できません。
※ 弊社製無線LANカード(SL-5000XG、SL-5100、SL-5200、SL-5200W、SL-5300W)をご使用になるときは、Card Bus対応のPCカードスロットを装備するパソコンをご用意ください。
※ 今後弊社から発売される無線LAN製品については、弊社サポートセンターにお問い合わせください。

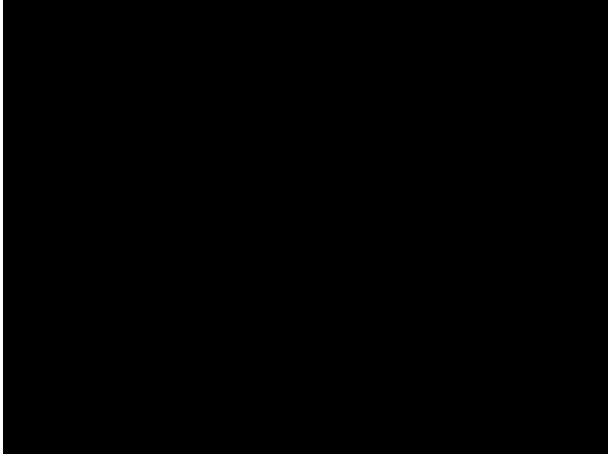
7. 暗号化対応表

弊社製の対応無線LAN製品で使用できる暗号化方式は、下記のとおりです。

暗号化方式 / 無線LAN製品	なし	WEP RC4			TKIP	AES
		64bit	128bit	152bit		
SL-11/SL-110	○	○	○	×	×	×
SL-12/SL-120	○	○	○	×	×	×
SU-12	○	○	○	×	×	×
SL-5000	○	○	○	○	×	×
SL-5000XG	○	○	○	○	×	×
SL-5100	○	○	○	○	×	×
SL-5200	○	○	○	○	○	○
SL-5200W	○	○	○	○	○	○
SL-5300W	○	○	○	○	○	○
SE-50/SE-50W	○	○	○	○	○	○
SE-56W	○	○	○	○	○	○
SE-80/SE-80M	○	○	○	○	○	○
SU-50W	○	○	○	○	○	○
SU-80	○	○	○	○	○	○

※通信相手と暗号化方式や暗号化ビット数が異なるときは、通信できません。
※本製品は、「OCB AES 128bit」に対応していません。
※本製品の[IEEE802.11n]規格は、暗号化方式を「なし」または「AES」に設定している場合に有効です。
※Windows XP、Windows Vista標準のワイヤレスネットワーク接続は、「WEP RC4 152bit」に対応していませんので、弊社製無線LAN製品に付属の設定ユーティリティーをご使用ください。
また、弊社製無線LAN製品に付属の設定ユーティリティーの場合、「TKIP」/「AES」に対応していませんので、Windows XP、Windows Vista標準のワイヤレスネットワーク接続をご使用ください。

高品質がテーマです。



A-6707-3J-①
© 2008–2009 Icom Inc.

アイコム株式会社
547-0003 大阪市平野区加美南1-1-32